NIBM WORKING PAPER SERIES

(Policy Research Paper)

New RBI Guidelines on Fraud Risk Management: A Risk Based and Data-Driven Approach

Smita Roy Trivedi
Aditi Kakade

Working Paper

(WP49/2024)

NATIONAL INSTITUTE OF BANK MANAGEMENT
Pune, Maharashtra, 411048
INDIA
December 2024

The views expressed herein are those of the authors and do not necessarily reflect the views of the National Institute of Bank Management.

NIBM working papers are circulated for discussion and comment purposes. They have not been peer-reviewed or been subject to the review for Journal or Book Publication

© 2024 by Smita Roy Trivedi and Aditi Kakade

Citation Guideline:

Roy Trivedi, Smita and Aditi Kakade (2024), "New RBI Guidelines on Fraud Risk Management: A Risk Based and Data-Driven Approach". NIBM Working Paper Series: Policy Research Paper WP 49/December.

https://www.nibmindia.org/static/working_paper/NIBM_WP49_SRTAK.pdf

New RBI Guidelines on Fraud Risk Management:
A Risk Based and Data-Driven Approach

Smita Roy Trivedi and Aditi Kakade

NIBM Working Paper No. 49
December 2024

ABSTRACT

In the context of the 'Internal Risk Assessment Guidance for Money Laundering/Terrorist Financing Risks' issued by Reserve Bank of India on October 10th, 2024 which focus on a risk based and data driven approach on fraud monitoring, we argue why the need for a risk-based system and why banks must quickly revamp their systems to optimise the use of internal and external data to develop more scientific risk rating models to be able to contain risk of frauds in their future business.

Key words: Fraud risk, data-driven system, money laddering

Smita Roy Trivedi (Corresponding Author)
National Institute of Bank Management
smita@nibmindia.org

Aditi Kakade
National Institute of Bank Management
ankakade@nibmindia.org

New RBI Guidelines on Fraud Risk Management:
A Risk Based and Data-Driven Approach

I. Background

The 'Internal Risk Assessment Guidance for Money Laundering/Terrorist Financing Risks' issued by Reserve Bank of India on October 10th, 2024 focus on a risk based and data driven approach on fraud monitoring. In this article we argue why the need for a risk-based system and why banks must quickly revamp their systems to optimise the use of internal and external data to develop more scientific risk rating models to be able to contain risk of frauds in their future business.

The Indian banking system, in sync with global experience, is grappling with the issue of increased frauds and heightened money laundering concerns. RBI Annual Report, 2023-24, shows that the total number of fraud cases (reported) has jumped from 13564 in 2022-23 to 36075 in 2023-24: a jump of 165%. Though from 2022-23 to 2023-24 amount involved in frauds has fallen by around 47%, it still amounts to Rs 13,930 crore (RBI Annual Report, 2023-24), with the sheer number of frauds affecting the banking system being staggering. The growing number of frauds and its changing dynamics of fraud are both a cause of concern for the banking system.

Two major sources of frauds in the Indian banking industry are internet-based frauds and credit frauds. RBI Annual Report 2023-24 points out that for private sector banks frauds have occurred predominantly in the category of digital payments (card/internet), while for public sector banks the credit frauds continue to be most dominant. As shown in Chart 1, the quantum of frauds from credit cards or internet banking have increased significantly from 0.1% in 2018-19 to 10.5% in 2023-24. The number of digital frauds has also increased substantially from 27.45% in 2018-19 to around 81% in 2023-24. Addressing fraud in online banking necessarily requires a commitment to the IT infrastructure optimal functioning. Chart 2 shows the quantum and number of credit of frauds as percentage of total frauds. While the number of credit frauds have fallen from 53% in 2018-19 to 11.5 % in 2023-24, the quantum has fallen only marginally from 90.2% in 2018-19 to 84.5% in 2023-24. Data driven approach is especially useful for given the differential impact on different fraud types on the banking system. Banks have internal data which can be a rich source of information on the build up to the fraud, early signals and transactions alerts. Mining data and qualitative information is essential for the banks to optimise the use of existing data. For transaction-based frauds, the bank's own historical data is crucial as transactional frauds like digital frauds vary according to its nature of business and exposures.

An analysis of the vintage of frauds shows the long-drawn nature of the frauds (chart 3). In FY 2022-23, new frauds reported in the current year contributed about 6% to the total value of frauds reported till date whereas the similar contribution of fresh frauds in FY 23-24 increased to 10.8%. It shows that the present measures adopted by Banks to deliver good quality credit are not adequate to contain new frauds and thus warrant more methodical tools which would facilitate risk based analytical method to

analyse and contain risks of frauds in future business by drawing analogies from the historical experience of the respective bank. Especially in the context of credit frauds, long gestation periods of the credit frauds require new approach to its management.

With the advent of technologies like Artificial Intelligence and Machine Learning, it is possible for banks to not only set up transaction-based alerts for frauds, but also to use technologies like Natural Language Processing to understand better early warning signals to fraud. Natural Language Processing (NLP) tools help to analyse documents, both internal and external, to understand the early signals to fraud. This is especially important for credit frauds, because credit frauds have a gestation period with early warnings building up over time which are subjective and majorly qualitative (Roy Trivedi, 2024).

To give an example, over the course of the bank's overall relationship with a particular company through its account, various observations and analysis about the company is made in internal documents of the bank. The bank also collects information on the company from external sources, collated by the bank in documents. This information is qualitative in nature but very rich as many observations about the firm, say triggers of events of default, factors leading to stress in account, complexity of inter group transactions etc. are recorded in such documents. With NLP tools, such documents can be analysed optimally to develop an understanding of early warnings to fraud/defaults and calculate quantitative estimates of fraud likelihood.

[Chart 1]

[Chart 2]

If number of credit frauds have gone down and quantum(value) has remained at almost same level, that means either the ticket size of new frauds is large or the old cases with large ticket size are still unresolved.

[Chart 3]

II. The increased risks on money laundering and new guidelines

The concerns regarding money laundering are not merely the use of banking channels to launder dirty money but use of funds in terrorist financing and other illegal activities. The laundering process involves 'placement' of money earned through illegitimate means in bank accounts, the 'layering' of such funds through movement in various accounts, and finally an integration into the formal economy through use of such money in legitimate transactions.

While banks and financial institutions have a comprehensive list of early warning systems that they must follow, banks often find themselves facing a trade-off between business growth and compliance. The early warning systems given by Reserve Bank of India and globally by FATF are many and often the resources required by the banks for being abreast on the guidelines can be onerous.

It is here the RBI's insistence on the use of risk-based assessment system becomes pertinent. While risk-based assessments have been part of FATF and Prevention of Money Laundering (PML) guidelines, the focus in the new guidelines will help banks to evaluate

the new credit proposals more logically based on its own internal experience with existing portfolio after giving appropriate weightage to various risk factors apparent in the proposal.

Risk based assessment entails attaching differential weightage to the compliance as per the different risks attached to a particular compliance norm. For example, while KYC and customer due diligence is important is its own accord, in case of a customer engaged in international trade payments the risk is heighted. The KYC requirements or Customer Due Diligence to be followed for a customer with international trade exposure, for example, would include not only the inclusion documents like the proof of business, IEC (Import export code) but also a continuous monitoring of his business activities and international transactions. Risk based approach allows the optimisation of resources as pragmatically speaking, compliance has a cost and banks do face a trade-off between business growth and a cautious approach based on early warnings from existing portfolio.

III. The new approach: measurement of fraud risk

The guidelines issued by the central bank gives a detailed methodology for working out the risk-based assessment system and how the bank's internal data can be garnered for this purpose. We use the example of trade based early warning list given in the appendix 1 as an example to explain the various steps given in the guidelines. The new approach as defined in the guidelines involves the following key steps:

1. Definition of the inherent risk factors (RF) and sub risk factors (SRF)

The risk factors can be 'customer risk factor', 'geographic risk factor', 'products, services and transaction risk factor', 'delivery risk factor' etc. The sub-risk factors (SRF) under the RFs can further be defined. For example, in assessing international trade transactions the risk factors have been identified in the trade template (Appendix 1) as:

- Product
- Profile
- Country
- Associates
- Pre-Shipping Check
- Other Checks

Again, within the category, various sub-risk factors like type of good, dual good characteristic, pricing range of goods, and kind of product are taken into account.

2. Collection of data on the RFs/SRFs

Here the bank must use its own and industry's historical transactional, quantitative and qualitative data. For example, based on its previous history of fraud/ money laundering cases, the bank can fetch data on how important a particular indicator is in money laundering activities. The over-invoicing and under-invoicing evidence of

cross border transactions of a borrower company and its resultant impact on quality of account can suggest how important the parameter of pricing range (of products sold by borrower entity) is for the bank as a whole and accordingly, the risk weights can be assigned. The total weightage for sub categories must add up to 1.

3. **Assignment of weights to the RFs/SRFs based on their contribution to the overall (enterprise-wide) ML/TF/PF risk.**

This means that for each of the categories of risk identified, we assign weights and sub weights as discussed in the previous section. For example, the category product has five factors each of which can be assigned weights based on internal and external data:

	Risk category: Product	*Weights*
Sub categories	Is it a Dual Good?	w1
	Is the pricing of 'similar items' not known?	w2
	Is there a range in pricing possible?	w3
	Is there a substantial range in pricing (possibility of very high value or low value for the good)?	w4
	Can the goods be used to hide other goods?	w5

Where , $\sum_{i=1}^{n} W = 1$

It is prudent for the bank here to make extensive use of their own data and industry data to derive the weights based on the past fraud instances.

4. **Assignment of weight ('Wi') to the risk factor (RFi) / sub-risk factor (SRFi) based on its risk posed by the particular RF/SRF**.

While RBI regulation mentions that assignment of weight may be based on expert judgement and/or considering the data relating to it, it would be advisable for banks to make the weights as " data driven" to the extent possible. It is prudent for the bank here to make extensive use of their own data and industry data to derive the weights based on the past fraud instances.

Final inherent risk ('IR') outcome for RF is defined as Inherent Risk for risk factor RFa (IR_RFa) :

IR_RFa = W1 * S_SRF1 + W2 * S_SRF2 + …

Where:

i Wi is the weight assigned to the sub-risk factor (SRFi) based on its risk *contribution*

ii S_SRFi is the score assigned to sub-risk factor SRFi. This score again may be based on the ML/TF/PF risk that it posed by the sub risk factor to the REs. For instance, if the RE takes a three-point scale, then score of 1 may be given in case of low-risk posed by the SRF, 2 in case of medium-risk and 3 in case of high-risk.

$\Sigma Wi = 100\%$

The weighted inherent risk score for each RF as calculated above again is to be mapped to appropriate risk levels viz., 'High', 'Medium' and 'Low' for calculating the 'inherent risk level'.

5. Identify and define the main control factors ('CFs')

The control factors which help mitigate and control the inherent risk of the concerned RF/ SRF should be identified. For instance, for RF 'product and services', the CFs may be 'policies and procedure', 'product approval process', etc. The guidelines suggest assigning weightage to each CF according to the importance it carries in mitigating and controlling the inherent risk of the particular RF, based on qualitative (expert judgement) and/ or quantitative evaluation.

The control factors can aim at both people risk elements and systems followed by the banks. According to the theoretical framework of fraud, the 'fraud triangle' developed by (Cressy, 1953) there are three specific dimensions or parts of fraud: pressure, opportunity and rationalization. 'Pressure' focuses on the forces that can make a person commit fraud, both external and internal like greed, need, extravagant living, preventing reputational damage, perceived injustice, and the quest for status (Schuchter. and Levi, 2016). The 'opportunity' aspect is the presence of situations or loopholes that allow a person to commit fraud which hints at presence of weakness within the 'fraud target' (Boyle, et al. 2015). 'Rationalization' points justification of moral transgression (Cressey, 1953) which is a 'permission' that fraudsters give themselves while committing the crime.

While nudges for ethical behavior of employees via training is theoretically sound, the bank cannot construct its entire fraud detection system primarily based only on the employee behavior for simple reason that many a times, the frauds are perpetrated by taking advantage of incapability of the bank officer to anticipate or detect the same. External and internal pressures to commit a fraud will remain and it is always possible to justify moral transgressions, so that it becomes very difficult to control these two aspects for prevention of fraud. 'Opportunity' for fraud refers to the gaps in systems and controls and is a function of corporate governance and internal systems. The opportunity aspect of the fraud triangle thus refers to the 'capability' to commit fraud given the 'systems'. A tighter system reduces the opportunities for fraud, making the bank less vulnerable to the moral transgressions as well as lack of expertise of its employees, so an optimum mix of both is essential.

It is in this context that the new guidelines assume importance. The process outlined involves assigning weighted scores to internal controls (e.g., policies, procedures, product approval processes) to assess their effectiveness in mitigating risk for a specific risk factor (RF). The control effectiveness score is mapped to a three-point scale (Strong, Satisfactory, Weak). By applying this score to the inherent risk level, a residual risk (RR) is determined for each risk factor. A residual risk matrix is then used to finalize the residual risk score for each risk factor.

References

Boyle, Douglas M., De Zoort, F. Todd, Hermanson, Dana R. (2015), The effect of alternative fraud model use on auditors' fraud risk judgments, Journal of Accounting and Public Policy, 34 (6): 578-596.

Cressey, D. R. (1953). Other people's money: a study in the social psychology of embezzlement. Glencoe, IL: The Free Press.

Reserve Bank of India (2016-17), Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs (Updated as on July 03, 2017), https://rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=1047

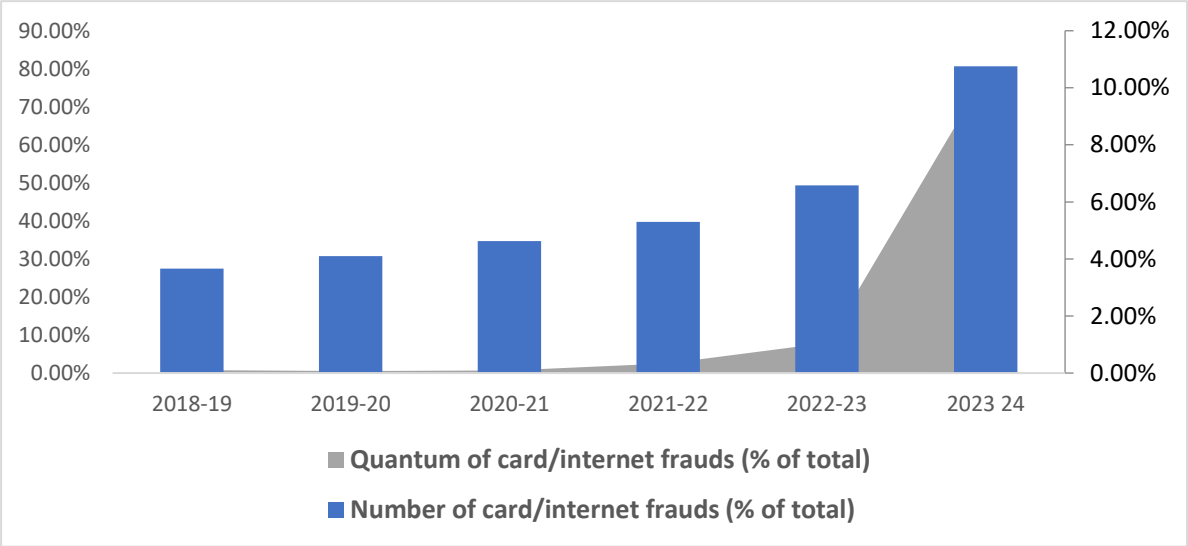
Reserve Bank of India (2020-21 – 2023-24), Annual Report, https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1377

Reserve Bank of India (10th Oct, 2024), 'Internal Risk Assessment Guidance for Money Laundering/Terrorist Financing Risks', https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=1278.

Roy Trivedi, Smita (Nov 17, 2024), RBI's new norms may help detect financial frauds, Hindu Business Line, https://www.thehindubusinessline.com/opinion/rbis-new-norms-may-help-detect-financial-frauds/article68879575.ece.

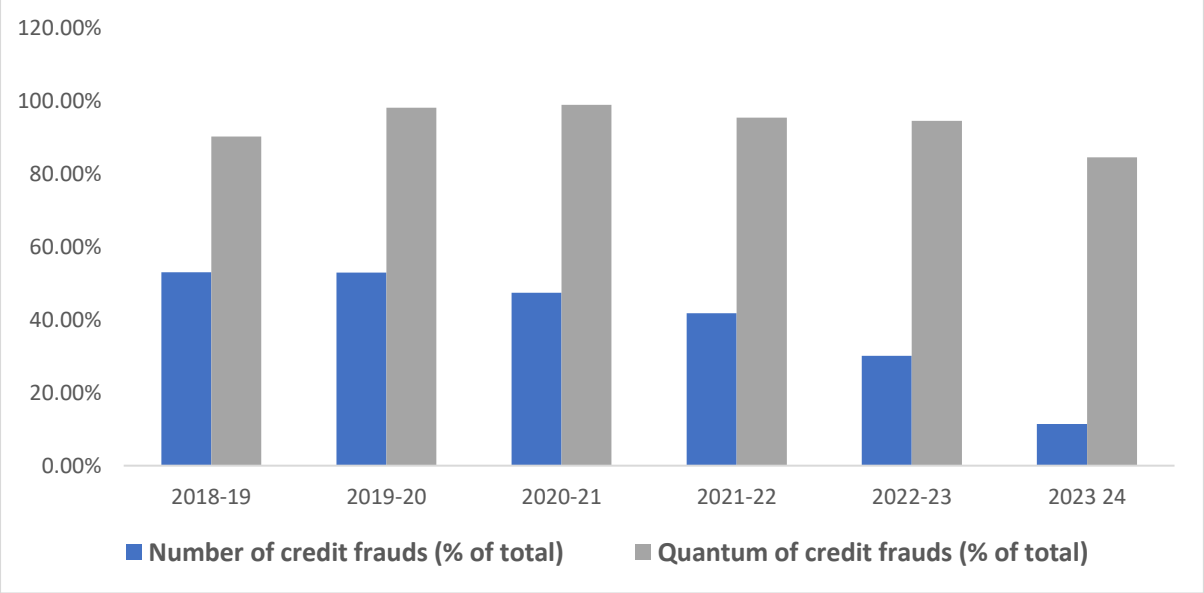
Schuchter, A. and Levi, M. (2016), The Fraud Triangle revisited. Security Journal, 29, 107–121 (2016). https://doi.org/10.1057/sj.2013.1

Chart 1
Quantum and Number of card/internet frauds (% of total)



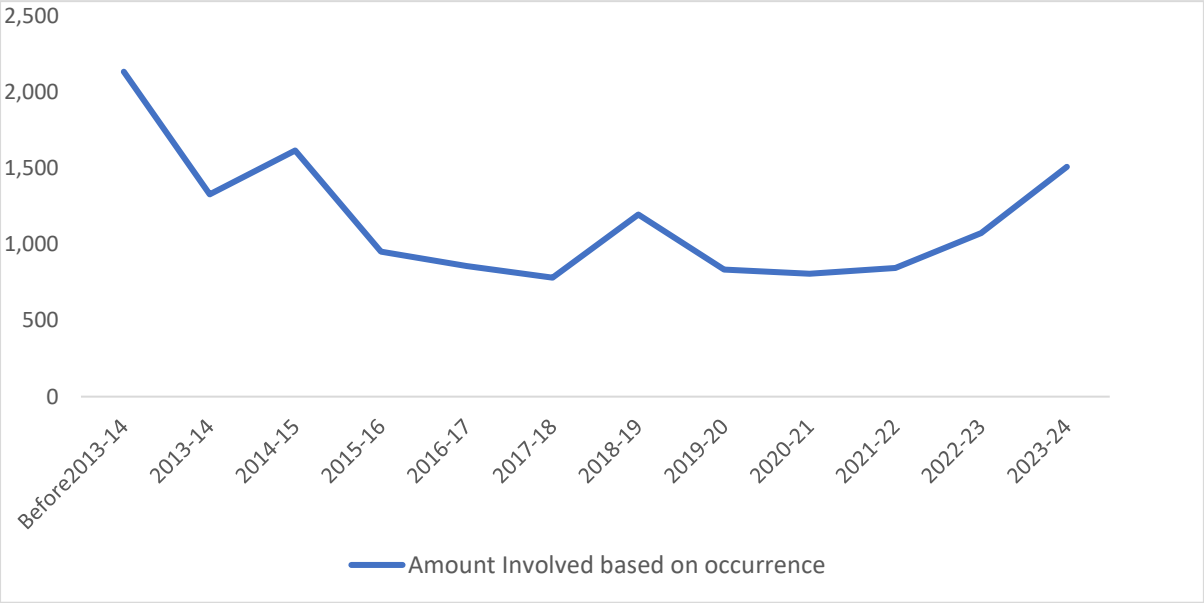
Raw data source: RBI Annual Report 2020-21 – 2023-24

Chart 2
Quantum and Number of credit frauds (% of total)



Raw data source: RBI Annual Report 2020-21 – 2023-24

Chart 3
Vintage of fraud reported in 2023-24 (Rs cr)



Raw data source: RBI Annual Report 2023-24

Appendix A

TEMPLATE FOR EARLY WARNING SIGNALS IN TRADE				
Smita Roy Trivedi				
A	**PRODUCT**	1	Is it a Dual Good?	
		2	Is the pricing of 'similar items' not known?	
		3	Is there a range in pricing possible?	
		4	Is there a substantial range in pricing (possibility of very high value or low value for the good)?	*
		5	Can the goods be used to hide other goods?	
B	**PROFILE**	1	Does the customer have less than two years relationship with bank?	
		2	Has the customer newly (in less than a year) changed his line of business?	
		3	Has the customer moved to a entirely different line of business?	*
		4	Does his/her reason for changing business activity not make economic sense?	
		5	Is KYC deficient with regard to international banking?	
		6	Does the customer have sister concerns?	*
		7	Are there substantial Intergroup transactions?	*
C	**COUNTRY**	1	Is the country high risk?	
		2	Is there a commodity country mismatch?	
D	**ASSOCIATES**	1	PRODUCT	Is it a Dual Good?
		2	PRODUCT	Is the pricing of 'similar items' not known?
		3	PRODUCT	Is there a range in pricing possible?
		4	PRODUCT	Is there a substantial range in pricing

				(possibility of very high value or low value for the good)?
		5	PRODUCT	Can the goods be used to hide other goods?
		1	Profile	Has the associate moved to a entirely different line of business?
		2	Profile	Does his/her reason for changing business activity not make economic sense?
		1	Country	Is the country high risk?
		2	Country	Is there a commodity country mismatch?
	PRE SHIPMENT - CHECK	1	Beyond capacity of Customer	
		2	Are there improbable goods/origins/quantities/destination?	
		3	Any concerns from A-1-5	
		4	Is there a unusual complexity in financing or a financial product used?	
		5	Is there transhipment through various locations without economic reason?	
		6	Is there an attempt to circumvent certain countries?	
		7	Has the LC been modified many times/ cancelled?	
		8	Is there last moment changes in payment instructions	*
		9	Are there third-party or unrelated party remittance for the transaction?	*

		10	Is there a third-party funding for the transaction?	*
		11	Are there RTGS to related parties regularly?	*
		12	Is the route logical?	
	OTHER CHECKS	1	Is there advance discrepancy waivers?	*
		2	Is the discrepancy waiver not making economic sense?	
		3	Are there discrepancies in description of goods?	
		4	Are there discrepancies in transport documents?	
		5	Are transport documents absent?	*
		6	Is there satisfaction of goods reaching destination?	