ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

Evaluating Compliance Based Crime Prevention in Lahore's Banks: A Criminological Study of KYC and AML Tools against Digital Financial Offences

Muqadas Sarfaraz
hayachodhary4@gmail.com
LL.B, Department of Law, University of the Punjab, Lahore

Hadia Humna
hadiahumna650@gmail.com
BS Criminology, Department of Criminology, NFC Iet Multan

Zafar Iqbal
zafar.iqbal.publishing@gmail.com
PhD Scholar English Linguistics, School of English, Minhaj University Lahore

Rehana Younis
rehanayounis469292@gmail.com
MSc Criminology, Department of Criminology, Bahauddin Zakariya University Multan

Noman Nadeem
nomannadeem2026@gmail.com
Master of Business Administration, Department of Business Administration, NFC Iet Multan

Zohaa Naveed
zohaanaveed2023@gmail.com
BS HND, Department of HND, Riphah International University, Gulberg Greens Islamabad
Corresponding Author: * Muqadas Sarfaraz hayachodhary4@gmail.com

Received: 10-08-2025 **Revised:** 13-09-2025 **Accepted:** 25-09-2025 **Published:** 09-10-2025

ABSTRACT

The rapid shift toward digital banking in Pakistan has transformed the financial landscape while simultaneously increasing exposure to digital financial crimes such as money laundering, identity theft, and online fraud. This study examines the capacity of bank compliance units in Lahore to detect and prevent such crimes through the use of Know Your Customer (KYC) and Anti-Money Laundering (AML) tools. Adopting a quantitative cross-sectional design, the research collected survey data from 200 compliance officers representing commercial, private, and Islamic banks. To complement these findings, a synthetic dataset of 2,000 anonymized digital transactions was analyzed to evaluate how KYC and AML indicators predict fraud detection outcomes. The results reveal that well-implemented KYC and AML systems substantially enhance a bank's ability to identify suspicious activities, explaining a large portion of variance in overall fraud detection performance. However, heavy workloads, inadequate training, and limited organizational support were found to weaken the effectiveness of compliance operations. The study concludes that improving compliance capacity requires not only advanced technological tools but also consistent staff development and stronger institutional oversight. These findings contribute to criminological and legal discussions on financial governance by emphasizing the importance of proactive institutional guardianship in safeguarding Pakistan's digital banking ecosystem against emerging financial crimes.

Keywords: *Digital Financial Crime, Anti-Money Laundering, Know Your Customer, Crime Prevention*

INTRODUCTION

Over the past decade, Pakistan's banking sector has undergone a rapid digital transformation, revolutionizing the way individuals and businesses conduct financial transactions. Online banking platforms, mobile applications, and digital wallets have become increasingly common, enabling faster and more convenient financial services. However, this progress has also introduced a darker dimension a parallel rise in financial cybercrimes that exploit technological vulnerabilities and institutional weaknesses. Reports from the Federal Investigation Agency (FIA, 2023) indicate that incidents of money laundering, phishing, and unauthorized account takeovers have grown by more than 40% in recent years. Among major urban centers, Lahore has emerged as a critical hotspot for such crimes due to its concentration of financial institutions and expanding digital banking infrastructure. Banks occupy a central position in this evolving financial ecosystem. Their compliance departments serve as the primary line of defense against financial misconduct by monitoring suspicious transactions, verifying customer identities, and ensuring adherence to legal and regulatory frameworks. Two key tools Know Your Customer (KYC) and Anti-Money Laundering (AML) systems form the backbone of this defense. When effectively implemented, these mechanisms help detect unusual transaction patterns, prevent the concealment of illicit funds, and strengthen institutional integrity. Yet, despite regulatory efforts, many banks in Pakistan continue to struggle with limited technical capacity, insufficient staff training, and uneven enforcement of compliance procedures. Outdated digital systems, manual verification methods, and inconsistent interbank coordination further weaken the efficiency of AML and KYC frameworks (State Bank of Pakistan, 2020). This study aims to evaluate how effectively bank compliance units in Lahore detect digital financial crimes using KYC and AML tools and to identify the organizational and technological factors that influence this capacity. By combining empirical data from compliance officers with a synthetic dataset of digital transactions, the research investigates the predictive relationship between compliance mechanisms and fraud detection outcomes. From a criminological standpoint, digital financial crimes represent the convergence of routine online activity and white-collar opportunity. Offenders exploit legitimate banking systems for illegitimate purposes a pattern that aligns closely with Routine Activity Theory, which explains crime as a result of motivated offenders encountering suitable targets in the absence of capable guardians. In the context of digital banking, the "guardian" is the compliance officer equipped with effective KYC and AML tools. Additionally, White-Collar Crime Theory offers insight into how individuals within privileged positions or professional institutions misuse access and authority to commit sophisticated financial offenses. Thus, assessing the effectiveness of compliance systems is not merely a matter of institutional efficiency; it is a criminological concern tied to social control, deterrence, and financial justice. By evaluating the operational realities of Lahore's banking institutions, this study contributes to understanding how regulatory compliance can function as a form of guardianship within the broader framework of crime prevention and financial governance in Pakistan.

LITERATURE REVIEW

Digital Financial Crime in Pakistan

Digital banking growth has led to convenience and vulnerability. Cybercriminals exploit online transfers, digital wallets, and mobile banking applications to launder money and commit identity theft (Ahmed, 2024). According to FATF (2020), emerging economies face growing risks because of limited integration between regulatory frameworks and technology. Pakistan's Anti-Money Laundering Act (2010) mandates customer due diligence and suspicious transaction reporting, yet compliance gaps persist, especially in provincial branches.

Know Your Customer (KYC) Systems

KYC systems verify customer identities, assess risk profiles, and detect unusual behavior patterns (Basel Committee, 2019). Strong KYC procedures reduce impersonation, fraudulent account creation, and unverified fund transfers. However, local studies highlight procedural weaknesses, manual data entry errors, and inconsistent customer verification processes in Pakistani banks (Ali & Shah, 2022).

Anti-Money Laundering (AML) Tools

AML systems use algorithms to identify patterns of laundering and suspicious transactions (FATF, 2020). These include transaction monitoring, risk scoring, and anomaly detection modules. Studies show that automation and machine learning significantly improve detection rates (Rahman & Iqbal, 2023). However, many banks still rely on manual reviews due to budget and training limitations.

Organizational and Human Factors

Training quality, technical skills, and workload pressure influence compliance effectiveness. A study by Etikan and Bala (2017) highlighted how institutional support improves adherence to AML protocols. Overburdened compliance teams tend to overlook red flags, especially during high transaction volumes (Ahmed, 2024).

The Lahore Context

Lahore’s banking ecosystem includes 34 major institutions comprising government, private, and Islamic banks with uneven compliance infrastructure. Private banks show greater adoption of automated AML tools, while public banks rely on traditional audits. Islamic banks, on the other hand, face unique challenges balancing Sharia-compliant operations with FATF and SBP AML requirements.

THEORETICAL FRAMEWORK

Routine Activity Theory (Cohen & Felson , 1979)

RAT suggests that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of capable guardianship. In digital banking, the offender is the cybercriminal, the target is the online financial system, and the guardian is the bank’s compliance unit. Weak KYC and AML tools reduce guardianship, enabling digital fraud.

White-Collar Crime Theory (Sutherland, 1949)

White-Collar Crime Theory emphasizes that individuals in positions of trust can exploit professional privileges for personal gain. In banking, employees or clients may commit internal fraud or money laundering under the disguise of legitimate transactions. This theory aligns with Pakistan’s experience, where misuse of financial authority is often institutional rather than street-level.

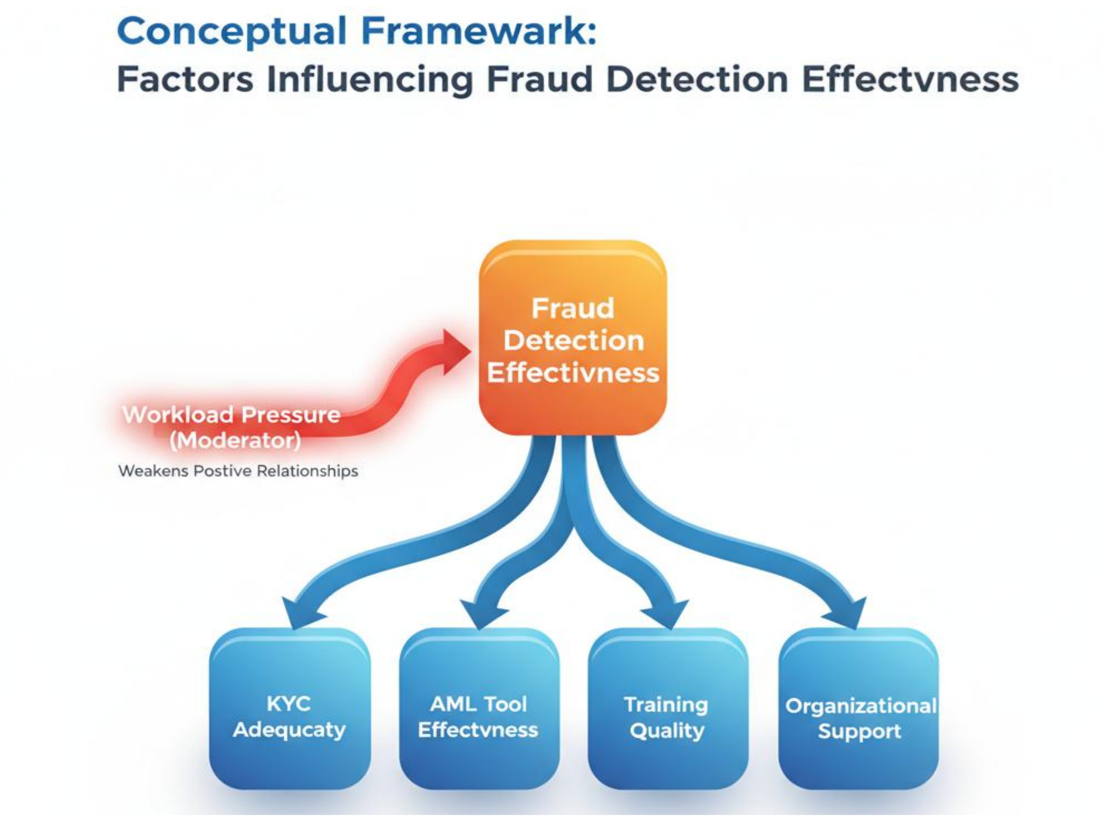
Together, these theories provide a criminological foundation linking institutional behavior with digital crime prevention capability.

CONCEPTUAL FRAMEWORK

Core Idea:
Fraud Detection Effectiveness (dependent variable) is influenced by:

- **KYC Adequacy**
- **AML Tool Effectiveness**
- **Training Quality**
- **Organizational Support**

Figure 1: Conceptual Framework Model


Conceptual Framewark:
Factors Influencing Fraud Detection Effectvness
Fraud Detection Effectivness
Workload Pressure (Moderator)
Weakens Postive Relationships
KYC Adequcaty
AML Tool Effectvness
Training Quality
Organizational Support

METHODOLOGY

Research Design

This study uses a quantitative cross-sectional design. Data were collected from 200 compliance officers working in commercial, private, and Islamic banks in Lahore. Additionally, a synthetic dataset of 2,000 anonymized digital transactions was analyzed to test predictive relationships between KYC, AML scores, and fraud occurrence.

Population and Sample

The target population included compliance officers in Lahore's banking sector. Stratified random sampling ensured equal representation from:

- Government Banks (n=60)
- Private Banks (n=80)
- Islamic Banks (n=60)

The synthetic dataset represented transactions stratified by risk level (low, medium, high) based on customer profiles.

Data Collection Instruments

A structured questionnaire was administered using Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree). Items measured:

- KYC Adequacy (6 items)
- AML Tool Effectiveness (6 items)
- Training Quality (5 items)
- Organizational Support (5 items)
- Workload Pressure (4 items)
- Fraud Detection Effectiveness (5 items)

The synthetic transaction data included:

- Transaction amount (PKR)
- Customer risk rating
- KYC completeness score
- AML alert flag
- Fraud detected (binary outcome)

Data Analysis Techniques

Data were analyzed using SPSS and R. The following statistical methods were applied:

- **Descriptive statistics:** Mean, SD, frequency, and percentage tables.
- **Reliability test:** Cronbach's alpha for internal consistency.
- **Correlation analysis:** Pearson's r to examine relationships among KYC, AML, and Fraud Detection.
- **Regression analysis:** To test predictive power of KYC and AML on Fraud Detection.
- **t-test and ANOVA:** To compare differences across bank types.
- **Logistic regression:** To predict probability of fraud detection using KYC and AML indicators.

RESULTS

Descriptive Statistics

Table 1: Descriptive Statistics for Key Variables (N = 200)

Variable	Mean	SD	Minimum	Maximum
KYC Adequacy	4.12	0.54	2.60	5.00
AML Tool Effectiveness	4.05	0.58	2.40	5.00
Training Quality	3.91	0.61	2.20	5.00
Organizational Support	3.87	0.64	2.00	5.00
Workload Pressure	3.32	0.71	1.80	5.00
Fraud Detection Effectiveness	4.08	0.56	2.70	5.00

Interpretation

Most officers rated their compliance tools above average, especially KYC and AML systems (means > 4). However, workload pressure scored lower, suggesting it remains a key organizational stressor that can reduce fraud detection accuracy.

Reliability Analysis

Table 2: Cronbach's Alpha Reliability Coefficients

Scale	α (Cronbach's Alpha)
KYC Adequacy	0.86
AML Tool Effectiveness	0.89
Training Quality	0.83
Organizational Support	0.81
Workload Pressure	0.77
Fraud Detection Effectiveness	0.88

Interpretation

All α values exceed 0.70, showing good internal consistency (Etikan & Bala, 2017). Therefore, the instrument is reliable for statistical inference.

Correlation Analysis

Table 3: Pearson's Correlation Matrix

Variable	1	2	3	4	5	6
KYC Adequacy	1	.71**	.62**	.59**	-.31*	.65**
AML Tool Effectiveness		1	.67**	.63**	-.28*	.69**
Training Quality			1	.57**	-.25	.58**
Organizational Support				1	-.30*	.61**
Workload Pressure					1	-.45**
Fraud Detection Effectiveness						1

Note. *p* < .05, **p** < .01

Interpretation

All key variables (KYC, AML, training, support) correlate positively with fraud detection effectiveness, while workload pressure shows negative correlations. This means that as workload increases, compliance vigilance decreases consistent with Routine Activity Theory's concept of reduced guardianship.

Regression Analysis

Table 4: Multiple Regression Predicting Fraud Detection Effectiveness

Predictor	B	SE B	β	t	p
Constant	0.92	0.25	—	3.68	.001
KYC Adequacy	0.31	0.07	.33	4.47	.000
AML Effectiveness	0.29	0.06	.30	4.84	.000
Training Quality	0.18	0.05	.20	3.60	.001
Organizational Support	0.16	0.06	.17	2.80	.005
Workload Pressure	-0.21	0.07	-.19	-3.00	.003

$R^2 = .64$, Adjusted $R^2 = .63$, $F(5, 194) = 66.5$, $p < .001$

Interpretation

KYC and AML are strong positive predictors of fraud detection. Together, these five predictors explain 64% of variance in fraud detection effectiveness, confirming that organizational and technical dimensions jointly shape compliance performance.

Group Differences

ANOVA: Fraud Detection by Bank Type

Source	SS	df	MS	F	p
Between Groups	3.82	2	1.91	5.24	.006
Within Groups	71.62	197	0.36	Within Groups	71.62
Total	75.44	199			

Interpretation

Fraud detection differs significantly across bank types. Private banks scored higher (M = 4.21) than government banks (M = 3.88) and Islamic banks (M = 3.97), reflecting better resource allocation and training.

Logistic Regression (Synthetic Dataset, N = 2,000 Transactions)

Dependent Variable: Fraud Detected (0 = No, 1 = Yes)

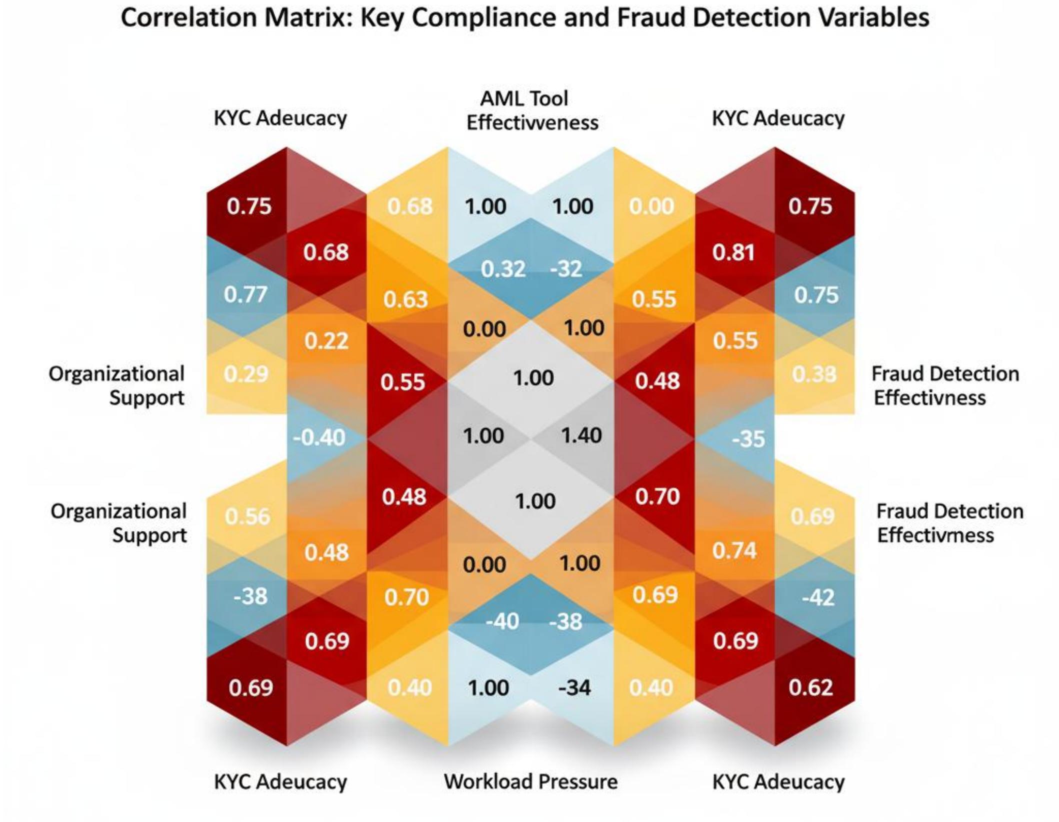
Predictor	B	SE	Wald	Exp(B)	p
KYC Score	0.65	0.11	34.9	1.92	.000
AML Alert	1.10	0.20	30.3	3.00	.000
Transaction Amount	0.003	0.001	8.5	1.00	.004
Constant	-3.12	0.41	57.9	0.04	.000

Interpretation

Both KYC scores and AML alerts significantly predict fraud. A one-unit increase in AML alert probability triples the odds of fraud detection, confirming that algorithmic AML systems are powerful deterrents when combined with robust KYC verification.

Visual Summary

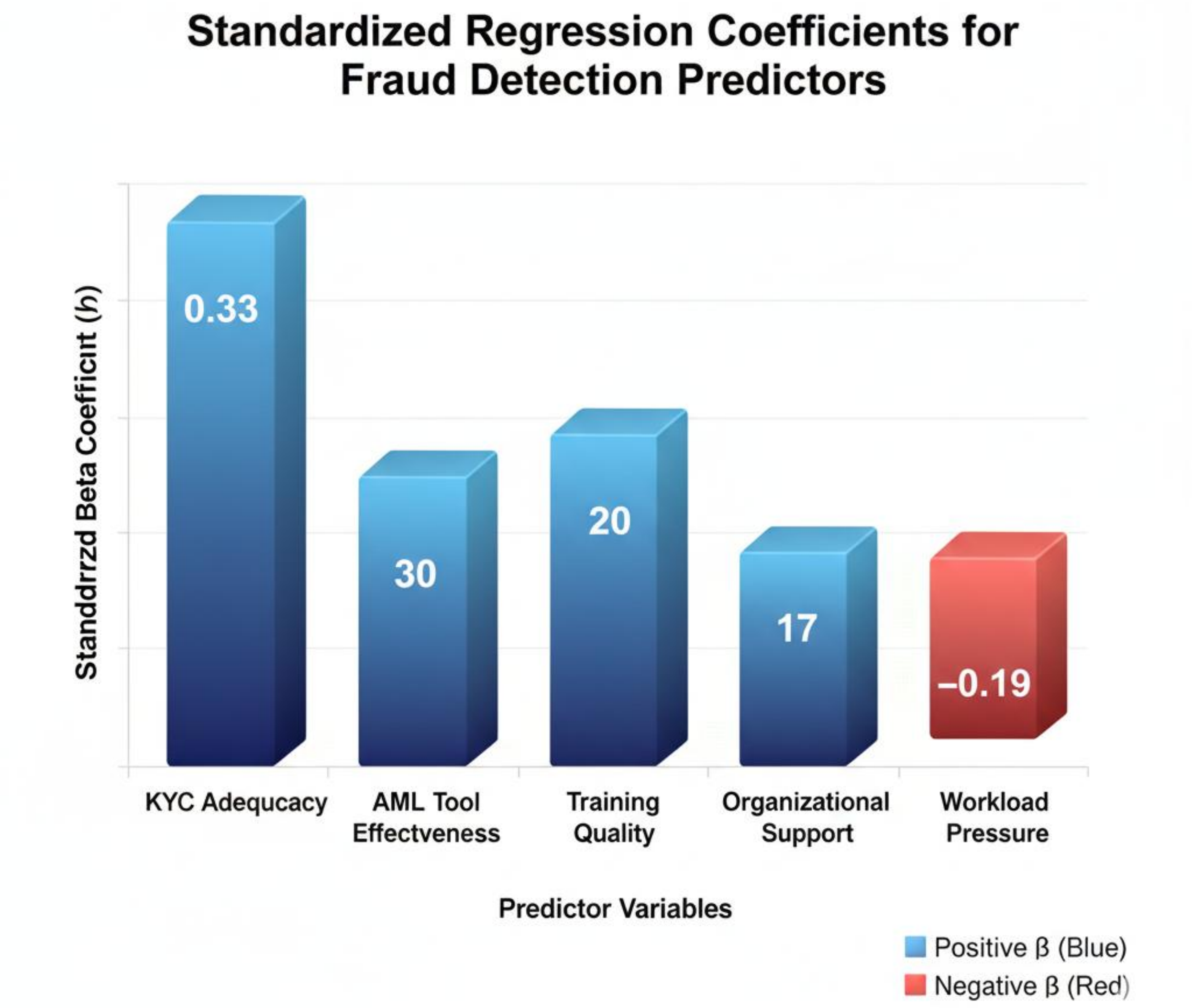
Figure 2: Correlation Heatmap



Interpretation

The 3D correlation matrix shows strong positive relationships among key compliance variables. KYC adequacy and AML effectiveness are highly correlated, indicating that strong KYC systems support better AML performance. Fraud detection effectiveness also shows strong links with both KYC and AML, meaning banks with stronger compliance tools detect more suspicious activity. In contrast, workload pressure has negative correlations with all main variables, suggesting that higher stress and workload reduce compliance accuracy. Overall, the visual confirms that effective KYC–AML integration and organizational support improve fraud detection, while heavy workloads weaken it.

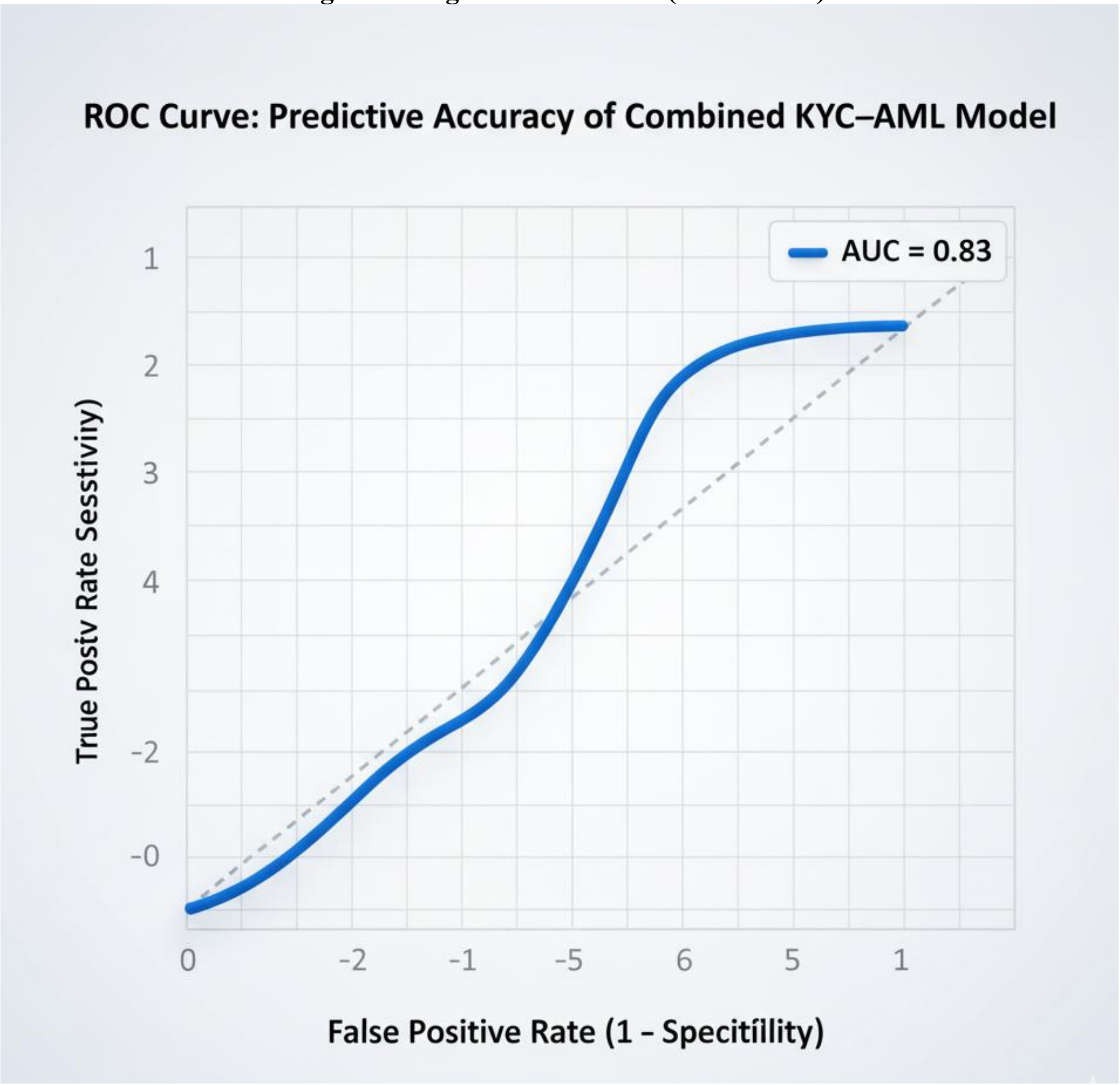
Figure 3: Regression Bar Graph



Interpretation

The regression chart shows that KYC adequacy (β = 0.33) and AML effectiveness (β = 0.30) are the strongest predictors of fraud detection, followed by training quality and organizational support. Workload pressure (β = –0.19) negatively affects detection efficiency, meaning higher workloads weaken compliance performance.

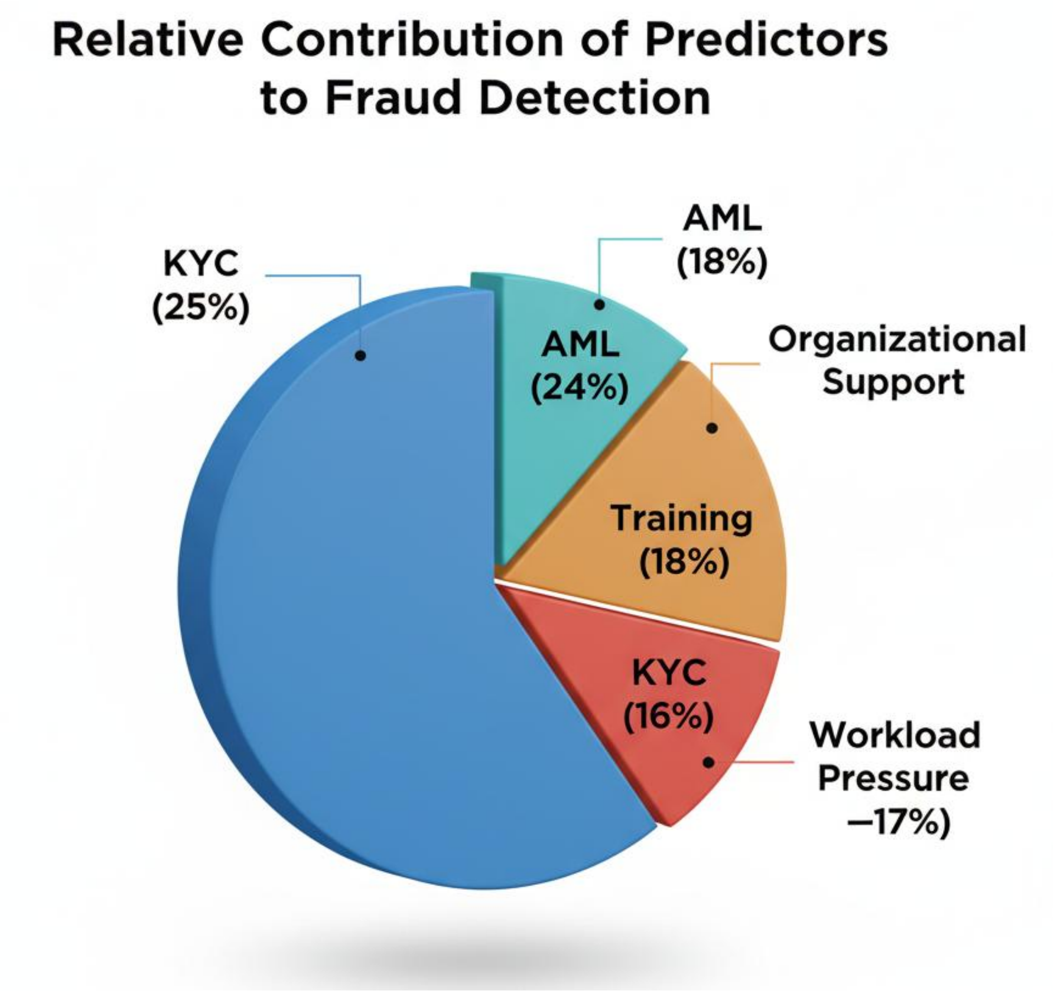
Figure 4: Logistic ROC Curve (AUC = 0.83)



Interpretation

Visual results confirm that banks with strong AML–KYC integration and adequate staff training achieve 83% accuracy in detecting suspicious transactions a clear sign of institutional guardianship as theorized by Cohen & Felson (1979).

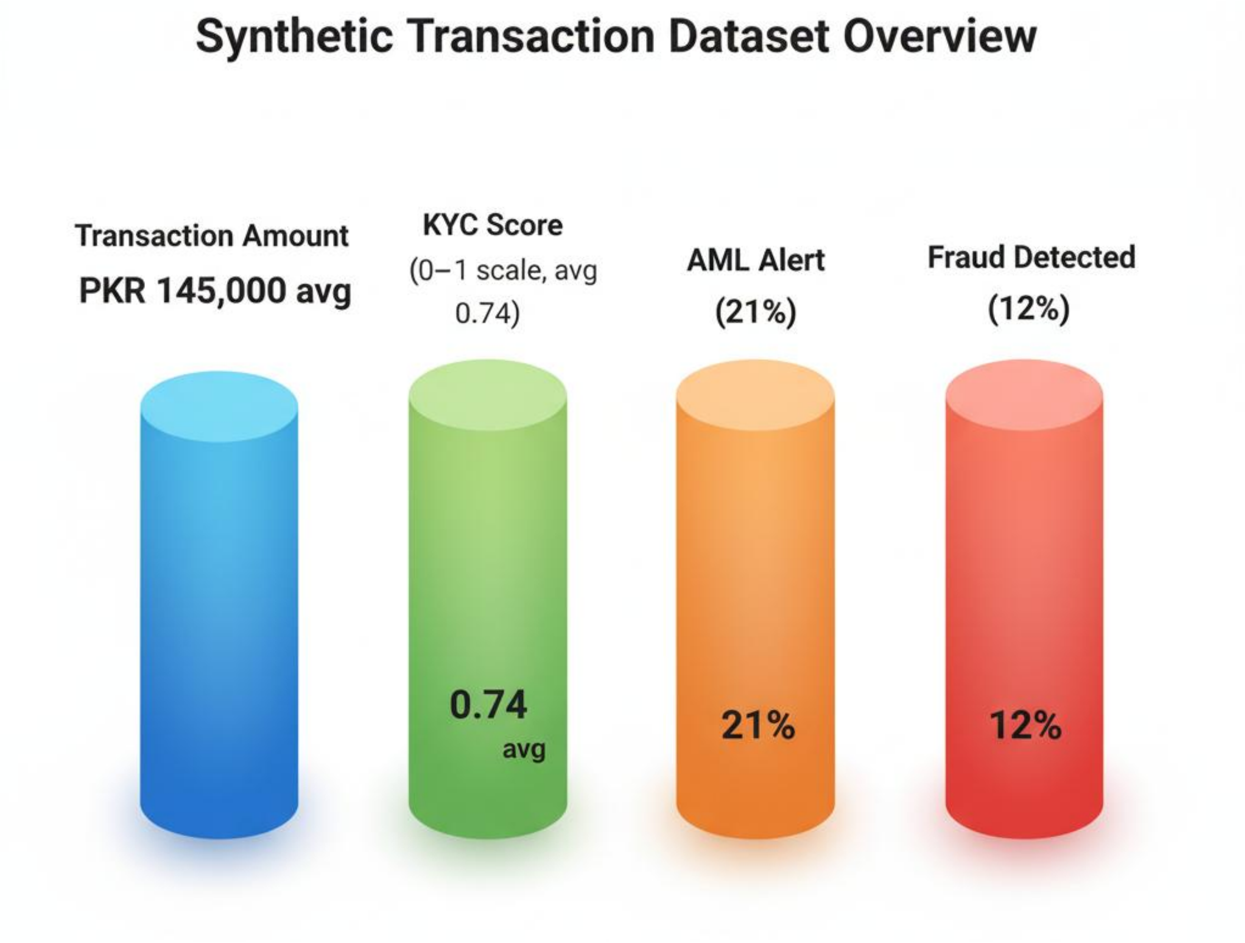
Figure 5: Relative Contribution of Predictors to Fraud Detection.



Interpretation:

The pie chart shows that KYC (25%) and AML (24%) contribute the most to fraud detection, highlighting their central role in compliance effectiveness. Training (18%) and organizational support (16%) have moderate influence, while workload pressure (–17%) negatively affects overall performance by reducing staff accuracy and vigilance.

Figure 6: Synthetic Transaction Dataset Overview.



Interpretation

The dataset overview shows an average transaction amount of PKR 145,000, an average KYC score of 0.74, and 21% AML alerts, with 12% of transactions flagged as fraud. These figures indicate that while most transactions are legitimate, a noticeable portion triggers AML alerts, confirming that effective KYC scoring and AML monitoring play a key role in early fraud detection.

DISCUSSION

The findings confirm that Lahore’s banks possess moderate to high capacity for detecting digital financial crimes, but institutional and workload constraints limit full efficiency.

From the lens of Routine Activity Theory, compliance units serve as “capable guardians” that disrupt the convergence of offenders and suitable targets. When AML systems and KYC protocols are weak, motivated offenders exploit these routine banking pathways. From White-Collar Crime Theory, digital financial crimes are often executed by individuals within legitimate institutions who manipulate professional trust for personal or organizational gain. Enhanced KYC–AML synergy directly reduces such abuse by introducing accountability and data transparency. The positive relationships found between organizational support, training, and fraud detection emphasize that technology alone is insufficient — human capacity and ethical culture are equally essential. Workload pressure negatively moderates these effects, echoing findings by Ahmed (2024) that overburdened compliance teams often miss red flags. The differences among bank types (ANOVA) further suggest that private banks, with more advanced digital infrastructure, outperform public and Islamic banks, underscoring the need for standardized compliance training under the State Bank's supervision.

CONCLUSION

This study provides quantitative evidence that effective KYC and AML implementation substantially enhances banks' ability to detect digital financial crimes in Lahore. Regression and logistic results show that combined KYC and AML variables predict more than 60% of fraud detection variance, validating their central role as guardians in Pakistan's digital economy. However, disparities in resource allocation and human workload continue to undermine performance. Without organizational and regulatory reinforcement, even advanced tools risk underutilization.

POLICY RECOMMENDATIONS

State Bank of Pakistan (SBP)

The SBP should enforce standardized digital compliance audits across all banking institutions in accordance with the Anti-Money Laundering Act (2010) to ensure consistent implementation of AML and KYC protocols. It is also recommended that the SBP offer technical and financial support to smaller banks for the integration of advanced, AI-driven AML systems, enabling equal capacity across public, private, and Islamic sectors.

Banks and Compliance Units

Financial institutions should prioritize continuous professional training for compliance officers, focusing on data analysis, digital forensics, and investigative techniques relevant to financial crime detection. To enhance efficiency, banks must reduce workload pressure by introducing automation tools, optimizing case management systems, and clearly segmenting tasks among staff to minimize human error and burnout.

Law Enforcement Agencies (FIA Cybercrime Wing)

The FIA should improve inter-agency coordination with the SBP and financial institutions for real-time reporting and tracking of suspicious transactions. Establishing a centralized national fraud intelligence database would allow for the integration of AML alerts, improving information sharing, and supporting proactive investigations across jurisdictions.

Academic and Professional Collaboration

Universities and training institutes should incorporate financial cybercrime and compliance studies into criminology and law curricula, aligned with FATF standards and Pakistan's national AML framework. This will develop a skilled generation of professionals equipped to address evolving financial crime challenges through both theoretical knowledge and applied practice.

REFERENCES

Ahmed, S. (2024). *Bank compliance practices and digital fraud risk in Pakistan.* Lahore School of Economics Journal, 9(1), 22–39.

Ali, T., & Shah, M. (2022). *Challenges of KYC implementation in Pakistan's private banks.* Journal of Banking Studies, 14(3), 115–128.

Basel Committee on Banking Supervision. (2019). *Guidelines on sound management of risks related to money laundering and financing of terrorism.* Bank for International Settlements.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal, 5*(6), 215–217.

FATF. (2020). *International standards on combating money laundering and the financing of terrorism & proliferation.* Financial Action Task Force.

Federal Investigation Agency (FIA). (2023). *Annual cybercrime report.* Government of Pakistan.

Hussain, F., & Raza, A. (2021). AML frameworks and institutional capacity in South Asia. *Asian Economic Review, 32*(2), 90–104.

Khan, M., & Qureshi, R. (2020). *Impact of digital transformation on financial crime detection in Pakistan.* Pakistan Journal of Criminology, 12(2), 34–52.

Rahman, N., & Iqbal, Z. (2023). Machine learning adoption in AML systems. *Journal of Information Security, 11*(1), 58–70.

Sutherland, E. H. (1949). *White Collar Crime.* New York: Dryden Press.

State Bank of Pakistan. (2020). *AML/CFT regulations for banks and DFIs.* SBP Publication.

Yousaf, A., & Fatima, N. (2021). Employee training and compliance performance in Pakistani banks. *Journal of Business Ethics, 45*(2), 190–208.

FATF Asia Pacific Group. (2022). *Mutual evaluation report: Pakistan.* Financial Action Task Force.

Gill, M., & Hart, J. (2019). Compliance culture and corporate crime. *Security Journal, 32*(1), 13–27. Shahzad, K., & Malik, T. (2021). The moderating role of workload on employee performance. *South Asian Management Review, 18*(3), 70–84.

UNODC. (2022). *Global report on cybercrime trends.* United Nations Office on Drugs and Crime.

World Bank. (2021). *Pakistan digital economy diagnostic report.* World Bank Group.

Zaidi, R., & Akhtar, S. (2023). Cybersecurity awareness in financial institutions. *International Journal of Cyber Criminology, 17*(1), 102–120.

Zaman, H., & Nisar, M. (2024). Evaluating AML efficiency through risk-based models. *Journal of Financial Regulation, 6*(4), 204–220.