ADVISORY NOTICE

NOTICE No: AF146/FIC/26/Vol.1/15

STRENGTHENING "KNOW YOUR EMPLOYEE (KYE)" CONTROLS TO MITIGATE INSIDER FRAUD, CASH THEFT AND STAFF-RELATED FINANCIAL CRIMES

Insider-related fraud, cash theft, suppression of customer funds, unauthorized transactions, document manipulation and other staff-related misconduct within the banking and financial sector is a major threat to integrity, stability and public confidence in financial institutions. Financial institutions are therefore advised to strengthen their "Know Your Employee (KYE)" frameworks as part of their enterprise-wide risk management, anti-fraud, AML/CFT/CPF and operational resilience programs.

This advisory seeks to:

- Alert financial institutions to the threat of insider fraud and employee misconduct.
- Encourage institutions to implement robust Know Your Employee (KYE) measures.
- Promote stronger internal controls, ethical culture and staff accountability.
- Enhance early detection and prevention of employee-enabled fraud schemes.
- Reduce operational, reputational, legal and financial risks arising from insider abuse.

KNOW YOUR EMPLOYEE (KYE)

Know Your Employee (KYE) refers to the processes and controls implemented by institutions to properly vet, monitor, assess and continuously evaluate employees throughout their employment lifecycle. KYE is an important complement to:

- Know Your Customer
- Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) controls.
- Fraud Risk Management frameworks.
- Cybersecurity and Information Security programs.
- Operational Risk Management systems.

An effective KYE program helps institutions identify employees who may pose elevated fraud, corruption, collusion, cybercrime or money laundering risks.

FRAUD RISKS OBSERVED

Financial institutions should pay particular attention to the following threat indicators and typologies:

Cash Theft and Suppression

- Unauthorized withdrawals
- Manipulation of teller balances
- Suppression of cash deposits
- Diversion of customer funds

Unauthorized System Access

- Abuse of privileged access rights
- Viewing or altering customer data without authorization
- Creation of fictitious accounts
- Circumvention of internal approval controls

Collusion and Syndicate Activity

- Staff collaboration with external fraudsters
- Facilitation of identity theft schemes
- Insider support for cyber-enabled fraud
- Leakage of customer credentials and sensitive data

Forgery, Camouflaging and Document Manipulation

- Alteration of account opening documents
- Forged signatures
- Manipulation of loans and credit records
- Fraudulent onboarding documentation

Lifestyle and Behavioral Indicators

- Sudden unexplained wealth
- Gambling or excessive debt problems
- Frequent override of controls
- Reluctance to take leave
- Close relationships with customers or vendors
- Excessive after-hours system activity

RECOMMENDED KYE CONTROL MEASURES

Financial institutions are advised to implement the following measures:

Pre-Employment Screening

Institutions should conduct comprehensive background checks before onboarding staff, including:

- Verification of identity and address
- Academic and professional qualification checks
- Employment history verification
- Criminal background screening where legally permissible
- Credit and financial standing checks for sensitive roles
- Reference checks from previous employers
- Sanctions and watchlist screening
- Social media and reputational assessments where appropriate

Special scrutiny should be applied to employees assigned to:

- Treasury operations
- Cash management
- Payments processing
- IT and Digital banking operations
- Compliance and audit functions

Risk-Based Staff Classification

Institutions should classify employees according to risk exposure and access levels.

High-risk categories may include:

- Tellers and cash officers
- IT administrators
- IT administrators;
- Operations personnel;
- Relationship managers;
- Payment processing officers;
- Staff with privileged system access.

Continuous Employee Monitoring

KYE should not end after recruitment. Institutions should implement:

- Continuous behavioral monitoring
- Periodic lifestyle audit
- Mandatory leave policies
- Access-rights reviews
- Transaction monitoring of staff-linked accounts
- Monitoring of unusual system activities

Automated monitoring systems should flag:

- Repeated failed login attempts
- Unauthorized access attempts
- High-value unusual transactions
- Dormant account activities
- Frequent reversals and overrides

Strengthen Internal Controls

Financial institutions should:

- Enforce segregation of duties to ensure no single employee has end-to-end control over critical transactions
- Implement maker-checker controls
- Introduce dual authorization for high-risk transactions
- Conduct surprise cash audits
- Enhance reconciliatory controls
- Maintain tamper-proof audit trails

Staff Ethics and Integrity Programs

Institutions should reinforce ethical culture through:

- Periodic integrity training
- Anti-fraud awareness programs
- AML/CFT compliance training
- Signed code of conduct declarations

Senior management should promote a "zero tolerance" policy toward fraud and misconduct.

Whistleblowing Mechanisms
Institutions should establish secure and anonymous reporting channels for:

- Insider fraud
- Corruption
- Suspicious employee conduct
- Ethical violations

Employees should be protected from retaliation when reporting misconduct in good faith.

G. Incident Response and Accountability
Financial institutions are encouraged to:

- Promptly investigate insider fraud allegations
- Report suspicious conduct to regulators and law enforcement agencies where appropriate
- Preserve audit logs and digital evidence
- Pursue disciplinary and legal actions against offenders
- Recover stolen assets where feasible

Failure to prosecute insider fraud may weaken deterrence and embolden future misconduct. Financial institutions are therefore strongly encouraged to strengthen their Know Your Employee (KYE) frameworks, enhance internal controls, improve employee screening and monitoring mechanisms and foster a culture of integrity, accountability and compliance.

A proactive and risk-based KYE regime remains a critical defense against insider threats, operational losses, financial crime and reputational damage.

ISSUED BY:
THE FINANCIAL INTELLIGENCE CENTRE
June 19, 2026.