

FRAUD, AI AND ACCOUNTABILITY

Protect money. Verify results. Act on warning signs.

Whether you lead an NGO, fund development programmes, run a business as a CEO or manage public funds, fraud threatens more than your finances. It can interrupt services, damage relationships and destroy confidence in your leadership.

These practical sessions will help you recognise warning signs, strengthen controls and respond effectively. Each session uses relevant cases and produces a tool or action plan participants can apply to reduce value leakage, and increase organisational value.

Virtual: free

Duration: 30 minutes.

Physical: free but you pay facilitation to trainers.

Duration: 1 hour.

Facilitation: UGX 500,000 per session.

After the Fraud Awareness Week fees:

Virtual / physical: Paid

Duration: 1 hour – 5 days

Fee per session per hour: USD 2,500, net of taxes.

No	Training topic	Who needs it most	Practical learning outcome
1	AI, Deepfakes and Digital Deception: Verify Before You Trust	All staff, executives, finance teams and business owners	Recognise impersonation risks involving cloned voices, fake videos and fabricated documents. Practise independently verifying requests before releasing money or confidential information.
2	Predictive Fraud Management: Use AI to Flag Risk Before Money Moves	Finance, risk, audit, procurement and technology teams	Develop a sample approach for scoring payment risk using transaction history, supplier information and approval patterns. Set clear thresholds for human review before payment.

3	The Enemy Within: Detect Employee and Management Fraud	CEOs, HR, finance, operations and internal audit	Identify payroll manipulation, false expenses, stock theft and management override. Build checks that address collusion and excessive access to systems and assets.
4	Fraud Red Flags and Internal Controls: Close the Gaps That Cost You Money	Department heads, supervisors and control owners across all sectors	Map a vulnerable process, identify where fraud could occur and strengthen its weakest controls. Leave with a checklist covering approvals, verification, access and reconciliation.
5	Speak Up Early: Turn Fraud Reports into Timely Action	All employees, boards, HR, compliance and investigation teams	Recognise reportable concerns, use appropriate reporting channels and handle allegations confidentially. Establish clear responsibilities for assessment, escalation and protection against retaliation.
6	Protect Every Payment: Mobile Money, Banking and Online Transaction Fraud	Businesses, SACCOs, NGOs, schools, finance teams and payment operators	Verify recipients, control payment approvals, recognise suspicious changes and reconcile transactions promptly. Practise responding when a payment goes to a suspected fraudster.
7	Protect Donor Funds: Verify Expenditure, Beneficiaries and Project Results	NGOs, implementing partners, project managers and grant accountants	Trace funds from approved budgets to actual delivery. Use data checks and AI-assisted matching to flag possible duplicate beneficiaries, double charging and unsupported expenditure for verification.
8	Conflicts of Interest, Bribery and Corruption: Expose Hidden Influence	Boards, public officials, procurement teams, NGOs and business leaders	Identify relationships and incentives that could compromise decisions. Apply disclosure, independent review and escalation procedures to supplier selection, recruitment, grants and approvals.
9	The CEO's Fraud Agenda: Protect Growth Without Weakening Accountability	CEOs, entrepreneurs, boards and senior management	Set clear fraud responsibilities, challenge management overrides and align incentives with responsible conduct. Develop a concise leadership dashboard that connects warning signs to decisions and action.
10	From Suspicion to Evidence: Investigate Effectively with AI	Investigators, internal auditors,	Preserve original records and use AI to help organise documents,

	Support	HR, compliance and legal teams	compare accounts and build an evidence-linked timeline. Verify every finding against its source before drawing conclusions.
11	The Profit That Is Not There: Detect Revenue and Financial Reporting Manipulation	Boards, CFOs, investors, lenders, funders and auditors	Compare reported performance with cash flows and supporting records. Identify unusual journals, unsupported revenue, concealed liabilities and adjustments that require further investigation.
12	The Invoice That Looked Genuine: Stop Phishing and Business Email Fraud	All staff, especially finance, procurement and executive assistants	Recognise manipulated payment requests, compromised email accounts and fraudulent supplier changes. Practise a verification process that works even when an email appears to come from a trusted person.
13	Healthcare Fraud: Protect Medicines, Claims and Patient Care	Health ministries, hospitals, clinics, insurers and health NGOs	Cross-check claims, treatment records, medicine issues and stock movements. Use analytics to flag repeated claims, unusual billing and unexplained shortages for targeted review.
14	Fraud in Education: Protect School Fees, Assets and Public Trust	School owners, governing bodies, headteachers, bursars and universities	Reconcile student records, fees, bank receipts, bursaries and payroll. Build practical checks against diverted collections, false refunds, procurement abuse and asset theft.
15	Procurement and Supplier Fraud: Verify the Bid, the Supplier and the Delivery	Government entities, NGOs, companies, procurement teams and project managers	Use document review and data analysis to flag suspicious awards, supplier relationships, pricing and contract changes. Strengthen checks that confirm goods and services were actually delivered.
16	Funder Assurance: Know Where Your Money Went and What It Achieved	Donors, foundations, development partners, grant committees and programme officers	Build a partner risk scorecard, verify reported results and target monitoring visits. Use evidence to guide funding decisions, additional checks and corrective action.
17	Growing Sales, Disappearing Cash: Find Fraud and Leakage in Your Business	Entrepreneurs, family businesses, retailers, manufacturers and distributors	Introduce a weekly owner's review of cash, stock, credit sales, discounts and refunds. Identify unexplained differences and assign follow-up without having to approve every transaction

			personally.
18	Public Money, Real Services: Detect Ghost Workers, False Beneficiaries and Undelivered Projects	Ministries, departments, agencies, local governments and public programmes	Link payroll, beneficiary, expenditure and delivery records to identify exceptions. Prioritise physical verification and assign responsibility for resolving unsupported payments.
19	Continuous Fraud Monitoring: Build an AI Early-Warning Dashboard	Risk, audit, finance, compliance and technology teams	Design a monitoring dashboard that combines rules and AI-generated risk scores. Assign alert owners, set response deadlines and measure useful detections, false alarms and unresolved cases.
20	Can You Trust Your Fraud Detection AI? Test It Before You Rely on It	Boards, executives, model owners, auditors and technology leaders	Test predictions against verified cases, assess missed fraud and false alerts, and check for unfair outcomes. Establish human review, secure data handling and regular reassessment as fraud patterns change.

Practical AI use throughout the programme

Participants learn how to use AI to prioritise suspicious transactions, compare records, identify unusual patterns and organise investigation material. AI alerts guide further review. People verify the evidence and remain accountable for decisions.

Choose the training that addresses your organisation's exposure.

Tell us your sector and your three biggest fraud concerns. We will help you select a focused session for your board, management or staff, built around the decisions they face and the controls they need to strengthen.

Let us work together to protect the funds, services and trust on which Uganda's growth depends.