CREATING A RESILIENT WORKFORCE AND CULTURE

Advancing internal investigative capabilities to stay ahead of emerging fraud risk areas

- Fostering advanced analytical and forensic techniques to enhance early identification of emerging fraud patterns.
- Deepening coordination between investigation, audit, and compliance teams for efficient and effective case resolution.
- Leveraging technology and behavioural insights to enhance the investigations accuracy and effectiveness.

Miguel Aguado

Vice President of Compliance
Ria Money Transfer | Xe.com
Euronet

FraudCon 2026

ria

Session Overview

01

The Fraud Landscape

Emerging patterns & why traditional controls fall short

02

Transaction Analysis

Cornerstone of early fraud identification

03

Three Lines of Defence

Integrated coordination for effective case resolution

04

Behavioural Insights

Human factors and AI-enhanced investigation accuracy

05

Graph Databases & Technology

Network analytics and emerging investigative tools

01

The Fraud Landscape

Emerging patterns & why traditional controls fall short

The Evolving Fraud Landscape

Why yesterday's controls cannot catch tomorrow's threats

↑ 43%

Rise in mule network complexity (Australian Cyber Security Centre (ACSC))

< 30s

Average time for a fraudulent transfer to complete

72%

Fraud now involves at least one digital channel

Emerging Risk Areas

Fraud Network Sophistication

Layered beneficiary chains and synthetic identities evade conventional node-level detection.

AI-Generated Social Engineering

Deepfake voices, cloned profiles and LLM-drafted scripts increase conversion rates for scammers.

Cross-Channel Coordination

Fraud orchestrated across crypto, remittance and banking rails within minutes.

Real-Time Payment Exposure

Instant settlement windows eliminate traditional manual review buffers.

ria Money Transfer

02

Transaction Analysis

The cornerstone of early fraud pattern identification

Transaction Analysis: The Cornerstone

Every fraud leaves a financial footprint — transactions are the evidence trail

"Transactions are the DNA of financial crime — patterns don't lie, even when people do."

Velocity & Frequency

Unusual spikes in transaction volume or frequency signal fraud activity and account takeover.

Beneficiary Patterns

Repeat or clustered beneficiaries across unrelated senders expose layering networks.

Behavioural Baseline

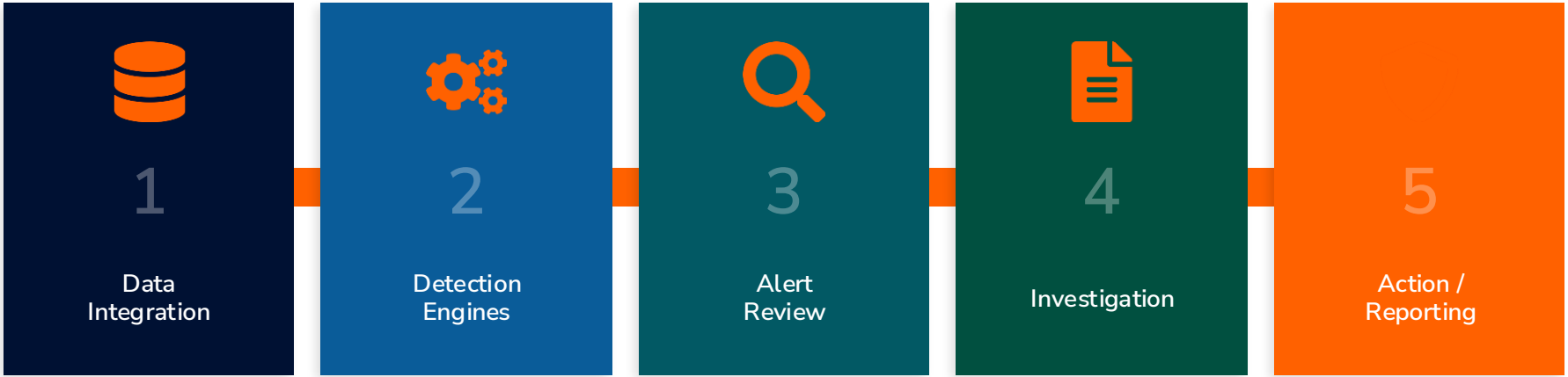
Deviation from established customer profiles triggers early-warning alerts before loss occurs.

Geographic Anomalies

Destination-country mismatch with customer profile — a leading fraud indicator in remittance.

The Transaction Intelligence Pipeline

From raw data to early fraud pattern identification



Key inputs at the Data Integration layer:

- Transaction history & frequency
- KYC / CDD records
- Device & channel signals
- Geographic & IP metadata
- Third-party watchlists

03

Three Lines of Defence

Integrated coordination between Investigation, Audit & Compliance

The Three Lines of Defence Model

Compliance as a shared, coordinated responsibility — not silos

1st Line

Business Operations

- Frontline fraud detection & real-time controls
- Customer interviews & immediate transaction decisions
- Block, cancel, escalate — with audit trail
- Primary data source for investigation teams

2nd Line

Compliance & Risk

- Policy governance and typology frameworks
- SMR / STR quality review & regulatory liaison
- Transaction monitoring rule calibration
- Cross-case pattern analysis and red flag libraries

3rd Line

Internal Audit

- Independent assessment of controls effectiveness
- Testing of detection engine performance
- Review investigation quality and timeliness
- Emerging risk horizon scanning

Deepening Cross-Team Coordination

Turning siloed investigations into a unified response machine

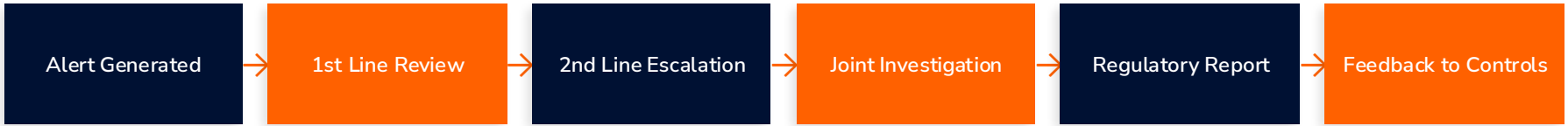
Common Friction Points

- ✗ Duplicate case work across investigation & compliance
- ✗ Intelligence not shared until STR / SMR filing
- ✗ Audit findings not looped into detection rule updates
- ✗ No unified case management timeline across teams

Coordination Best Practices

- ✓ Shared case management platform with unified timeline
- ✓ Cross-functional triage coordination
- ✓ Automated escalation triggers on threshold breaches
- ✓ Detection rule feedback loop — audit → controls update

Escalation & Information Flow



04

Behavioural Insights

Human factors and AI-enhanced investigation accuracy

Behavioural Insights & Investigation Accuracy

Understanding the human element — victim, mule, and fraudster behaviour

Victim Vulnerability Indicators

Age

Elderly customers disproportionately targeted — 68% of scam victims over 55.

Country of Birth

Australian-born sending to non-typical destinations — elevated risk profile.

New Customer

No transaction history + first-time send = heightened scrutiny required.

Consistency

Amount / frequency / beneficiary deviation from established baseline

The Investigator's Interview Framework

1. Did you perform this transaction?
2. Can you confirm the amount and beneficiary?
3. What is the purpose of this transfer?
4. What is your relationship with the beneficiary?
5. Do you know the beneficiary in person?

AI-Augmented Interview Insights

- Sentiment and hesitation pattern flags from voice/text channels
- Real-time script prompts based on detected fraud typology
- Automatic inconsistency detection across customer statements
- Risk score update after each interview data point collected

05

Graph Databases & Technology

Network analytics and emerging investigative tools

Graph Databases: Beyond Individual Transactions

Revealing hidden networks, relationships and criminal patterns

Capability	Traditional Systems	Graph Databases
Relationship detection	Limited — pairwise only	✓ Multi-hop, unlimited depth
Pattern complexity	Struggles with ring structures	✓ Detects layered mule rings
Visualisation	Tables / flat reports	✓ Intuitive network diagrams
False positive rate	High — rigid rules	✓ Contextual — lower noise
STR / SMR report quality	Narrative only	✓ Graph-supported evidence
Regulatory expectation	Reactive	✓ Proactive, intelligence-led

✦ *Graph analysis is now a regulatory expectation, not a differentiator — it is the baseline.*

ria Money Transfer

Graph Analysis in Practice

Case study: uncovering a structured mule network

How a Graph Investigation Works

01 Seed the graph

A flagged transaction or customer becomes the starting node.

02 Traverse relationships

Follow links — shared beneficiaries, devices, addresses, phone numbers.

03 Identify clusters

Automated community detection reveals rings and hub-and-spoke patterns.

04 Visualise & narrate

Graphical output supports STR quality and third-party communications.

Why Graph Databases Win

Comprehensive scope

Investigates beyond the individual — finds connected suspects and facilitators.

Intuitive visualisation

Criminal networks presented graphically for investigators and regulators alike.

Higher report quality

Graph evidence dramatically improves SMR / STR narratives and acceptance rates.

Proactive stance

Identifies emerging typologies before they reach material loss levels.

ria Money Transfer

Technology Stack for Investigative Excellence

Layered tools that amplify investigator judgment — not replace it

Graph Databases

Entity-relationship mapping, community detection, multi-hop traversal. Native fraud-ring visualisation.

Machine Learning Anomaly detection

Unsupervised models surface behavioural outliers. Reinforcement learning tunes alert thresholds over time.

Rules Engine + AI Hybrid detection

Deterministic rules catch known patterns; ML surfaces unknown ones. Together they close the detection gap.

Unified data repository

Single source of truth for historical pattern analysis. Enables longitudinal typology development.

Case Management Integrated workflow

End-to-end case lifecycle — alert to report. Collaboration layer across all three lines.

Questions & Discussion

"Compliance is everyone's responsibility."