
MERITRA BANKING • FRAUD OPERATIONS

Fraud & Scam Prevention Kit

Fraud is the #1 board risk in 2026.

This sample contains one of the three tabletop exercise scenarios (the Pix/APP Fraud Wave), preview of the CNBV 6-Behavior checklist, and the fraud risk appetite framework used by risk committees across tier-1 and tier-2 LatAm banks.

32 PAGES

PDF + 8-sheet xlsx

3 SCENARIOS

Pix • SPEI • USD

USD 149

One-time

Get the full kit at meritra.co/banking



Why fraud moved to #1

Bank Director's 2026 Risk Survey placed fraud and cyber at #1 and #2 on the CEO risk list for the first time. Themis Fraud Preparedness 2026 reports that two out of three banks describe themselves as "only somewhat prepared." The Pix wave in Brazil, ATO via SPEI in Mexico, and the USD wire desk threat in cross-border LatAm have consolidated fraud as the top operational risk CROs are answering for in 2026.

This kit gives a CRO, Head of Fraud Ops, or CISO the operational artifacts needed to answer the board: a fraud risk appetite framework, three tabletop exercise scenarios with scripted decision points, an incident response playbook, and the CNBV 6-behavior checklist operationalized for five LatAm jurisdictions.

What is in this sample vs. the full kit

| | Sample (this PDF) | Full Product |
|-------------------------------|-------------------|---------------------------------|
| Tabletop scenarios | 1 of 3 (Pix) | All 3 |
| Incident playbooks | 1 excerpt | 5 decision trees |
| Fraud risk appetite framework | Partial | 9-typology framework |
| CNBV 6-Behavior checklist | Preview | Full checklist + 5-country ext. |
| 14 fraud KPIs | — | xlsx with 8 sheets |
| Benchmark reference card | — | Included |
| Q&A prep pack | — | 30 board questions |
| Price | Free | USD 149 |



Scenario 1 - Pix APP Fraud Wave

A social-engineering campaign targeting 200+ customers in 48 hours with Pix transfers. The script below runs a 90-minute tabletop session with six defined roles. The other two scenarios in the full kit (ATO via SPEI in Mexico, and Insider Wire Desk Fraud USD) follow the same format.

Scenario briefing

Date: Monday, 07:00 local time. Your fraud ops center receives 187 alerts in 40 minutes. Customers report unauthorized Pix transfers ranging from BRL 500 to BRL 15,000. Early analysis suggests a phishing SMS campaign impersonating tax authority collection. Social media is amplifying. A journalist from Valor has called press relations. It is 07:42.

Decision points (first 90 minutes)

| Time | Decision | Primary owner |
|-------|---|-------------------|
| 07:42 | Activate Tier-2 fraud incident protocol — yes/no | Head of Fraud Ops |
| 07:50 | Push preventative block on outbound Pix to new recipients >BRL 1,000 | Head of Payments |
| 08:15 | Customer communication — SMS, app push, or both? | Head of Comms |
| 08:30 | Central bank + BCB Desaf notification — now or wait for confirmation? | CRO |
| 09:00 | Press line — confirm incident, defer to updates, or no comment? | CEO + Comms |



Operationalized for 2026

CNBV Circular 14/2021 requires banks to monitor six behavioral patterns. The full kit maps each behavior to a specific control, a monitoring metric, and a response procedure, plus extends to BCB Resolution 4.557 (Brazil), SFC Circular 029 (Colombia), BCRA Resolution A 7543 (Argentina), and SBS Peru equivalents.

Preview below: 2 of the 6 behaviors with full control mapping.

BEHAVIOR • 01

Transactions inconsistent with the customer's declared economic profile

Control: Real-time transaction screening against declared income bracket and profession. Threshold: transaction > 3x monthly declared income triggers review.

Monitoring metric: % of flagged transactions resolved within SLA (target: 95% within 24h). % of flagged that convert to SAR filing (expected: 8–12%).

Response procedure: Tier-1 analyst review. Escalation to Tier-2 if customer cannot justify within 48h. UIF/SAR filing decision within 72h of escalation.

BEHAVIOR • 02

Rapid movement of funds through multiple accounts without economic rationale

Control: Network analysis on accounts with ≥5 counterparties in rolling 7-day window. Detection of circular flows, mule account patterns, and layering.

Monitoring metric: Number of mule-account patterns identified per month. Time from first transaction in pattern to detection (target: <14 days). % of detections confirmed as mule activity (expected: 60–80%).

Response procedure: Immediate outbound transaction freeze on identified network. UIF notification within 24h. Coordinated takedown with receiving institutions.

In the full kit: The remaining 4 CNBV behaviors (structuring; cash-intensive business patterns; offshore transactions without rationale; PEP-connected flows), plus the 5-country extension matrix mapping each behavior to the equivalent regulatory citation in Brazil, Colombia, Argentina, Peru, and Chile.



9-typology framework

The fraud risk appetite framework defines thresholds for nine fraud typologies. Each threshold triggers escalation rules that link to the incident response playbook. The framework is used in practice at tier-1 LatAm banks as the standard language between the risk committee and the fraud ops team.

| Typology | Example threshold | Escalation |
|--------------------------------|---|-----------------------|
| APP fraud (social engineering) | Monthly loss > 0.8 bps of transacted volume | CRO |
| Card-not-present | Monthly loss > 15 bps of CNP volume | Head of Cards |
| Account takeover (ATO) | Weekly confirmed ATO cases > 50 | CISO + CRO |
| Insider fraud | Any confirmed case above USD 10k | Board audit committee |
| Synthetic identity | Monthly identified cases > 1% of new applications | CRO |
| Mule accounts | New mule accounts identified > 150/month | Head of Fraud Ops |
| [+ 3 more typologies] | In full kit | In full kit |



SECTI

LAUNCH PROMO

USD 149

WI

LAUNCH USD 14.90 - 90% off

• 32-p Through May 6, 2026 · 23:59 PT

Check After: USD 59 (60% off)

meritra.co/banking

• 8-sh

• 3 tabletop scenarios — Pix (Brazil), SPEI (Mexico), USD wire (Argentina)

• 5 incident decision trees — APP fraud · ATO · insider · mule network · vendor compromise

• Q&A; prep — 30 board/committee questions with primary-sourced answers

• Benchmark reference card — industry-standard fraud loss ratios by product line

• Lifetime updates as the regulatory landscape evolves

• 14-day money-back guarantee

Get the complete kit

meritra.co/banking · USD 149 · one-time · lifetime updates