Independent Rapid-Options Brief: Minimum Protections Against Bad Banking Actors

Prepared by: Vamakshi Chaturvedi*, MSc Economics – University of Manchester*
Date: 12 November 2025

---

1. Problem Snapshot

Municipal and partner banking networks face accelerating threats from fraud rings, mule accounts, synthetic IDs, and automated transfer abuse.
Because municipalities often operate under legacy systems and modest budgets, a **minimum viable protections** set is required—controls that are quick to deploy, low-cost, and compatible with existing infrastructure.

Recent **CFPB alerts** and municipal-banking data show that fraudulent digital transactions have risen by **over 30 percent year-on-year**, exposing public treasuries to substantial losses.

Key risk vectors include:

- Rapid account creation using reused devices or identities.
- Automated small-value drains exploiting delayed reconciliation.
- Social-engineering and benefit-payment diversions.
- Lack of centralized visibility across participating institutions.

---

2. “No-Regrets” Control Set (30–60 Day Deployment Window)

Category	Control	Expected Benefit	Effort / Cost
Onboarding	Duplicate-entity + device fingerprint check	Stops recycled IDs and shared devices	Low
Transaction rules	Velocity limits, new-payee cooling period (24 h), geo/IP mismatch alert	Prevents rapid fraud cascades	Medium
Behavioral flags	Round-dollar bursts, night-hour spikes, “first-use” anomalies	Detects scripted / bot activity	Low
Manual review queue	High-risk events held ≤ 24 h for human decision	Reduces false positives	Medium
Comms & UX	Just-in-time warning: “Confirm unusual transfer”	Reduces user-initiated fraud	Very Low

These measures rely only on rule-based logic—no machine-learning pipeline—and integrate easily into existing transaction-monitoring modules.

3. Minimum Data Needed to Enable Detection

Layer	Data Fields	Purpose
Onboarding	Customer ID hash, Device ID, IP, Employer / Benefit type, Funding source	Detect duplicates, build risk baselines
Transactions	Amount, Merchant/MCC, Timestamp, Location/IP, Payee novelty, Device match	Spot velocity and geo anomalies
Feedback Loop	Confirmed fraud labels	Train thresholds, measure precision

Data can be pseudonymized; only derived risk indicators need sharing across partners to remain privacy-compliant.

4. Fast Deployment Path

Week 1–2: Baseline dashboards + core rules (no model).
Week 3–4: Introduce risk scores (simple weighted rules).
Week 5–8: Tune thresholds; monitor KPIs (false-positive %, blocked loss, review SLA).

Deliverables:

- Excel / Sheet **Rules Register**
- Weekly **Risk Summary Dashboard**
- **Fraud Loss Avoided vs Customer Friction** chart

5. Success Metrics

Metric	Target
% high-risk tx caught pre-settlement	≥ 85 %
False-positive rate	≤ 10 %
Average review time	< 1 day
Blocked loss value	Consistent weekly decline
Customer friction reports	≤ 2 % of active users

6. Implementation Considerations

- **Governance:** Appoint a light **Fraud Ops Committee** (2 tech + 1 policy lead).
- **Privacy:** Apply hashed identifiers; share aggregates only.
- **Auditability:** Each alert logged with timestamp and rule trigger.
- **Scalability:** Same rule set extends to housing, benefit, and payroll platforms.

7. Conclusion

This brief outlines a set of **immediately deployable, non-disruptive safeguards** designed to reduce exposure to bad-actor banking patterns within public finance and government payment systems. The proposed rule-based controls**,** minimum viable safeguards**,** and data-lite detection mechanisms enable measurable protection within a short eight-week window, balancing **fraud deterrence** with **public-service delivery efficiency**.

The framework is intentionally simple, scalable, and operationally realistic. It can be adopted incrementally across **local, state, and federal programs**, supporting secure, ethical, and resilient automation in financial workflows. By combining practical detection logic with structured KPIs and governance routes, this brief demonstrates how **applied economic reasoning** can translate into actionable fraud-risk controls for real-world public finance contexts.

Appendix A – Risk Rules & KPIs (1 Page)

A.1 Risk-Rules Register (sample)

Rule ID	Rule Name	Threshold	Trigger Action	Owner
R1	New Payee Cooling Period	24 h	Hold tx until verified	Ops Team
R2	Velocity Cap	> 3 tx / 5 min	Flag + queue	Fraud Ops
R3	Geo/IP Mismatch	> 2 locations within 6 h	Alert	Tech Lead
R4	Device Reuse	Same device > 3 accounts	Block onboarding	KYC
R5	Round-Dollar Spike	≥ 10 tx exact $100	Review	Fraud Ops
R6	After-Hours Transfer	00:00–05:00 local	Warn + confirm	UX Team
R7	New Account Large Tx	> $5 000 in first 72 h	Manual check	Ops
R8	Duplicate Employer IDs	≥ 2 beneficiaries same hash	Review	Policy
R9	High-Risk Merchant MCC	List of codes	Queue	Risk Analyst
R10	Failed Login Bursts	> 5 attempts / 30 min	Temp lock	Security

A.2 Weekly KPIs Dashboard Template

KPI Category	Metric	Week 1	Week 2	Week 3	Trend
Detection Precision	% alerts confirmed fraud				→
Prevention Impact	$ loss blocked				→
False Positives	% non-fraud alerts				↓
Ops Efficiency	Avg review time (h)				↓
User Experience	Complaints / 100 tx				↔

A.3 Data Dictionary (Excerpt)

Field	Description
device_id	Unique hashed identifier per device
payee_novelty	Flag if payee first seen for user
txn_amount	Numeric transaction value
txn_time	UTC timestamp
mcc_code	Merchant category code
fraud_label	1 = confirmed fraud, 0 = legit

A.4 Notes

- The tracker and dashboard can be implemented in Google Sheets or Excel within one day.
- Fields are minimal to protect privacy; additional enrichment optional later.
- Regular weekly KPI reviews create a continuous feedback loop for tuning.