POLICY BRIEF | FRAUD INFRASTRUCTURE & ELDER PROTECTION

How Bank Outsourcing Creates the Infrastructure Scammers Exploit

Sherry Spurlin | Spurlin Digital Solutions | Licensed Mortgage Professional, 30+ Years Financial Services

THE PROBLEM

When Americans open a bank account, they believe their financial data is protected by the institution they trust. That assumption is increasingly false.

Major banks are quietly outsourcing core operations — including direct access to customer account systems — to third-party contractors operating in regions with documented fraud activity. No federal law requires disclosure of where these contractors are located. No law mandates real-time monitoring of their access. No whistleblower protection exists for the overseas employees who witness abuse.

$3.4B
Elder fraud losses (2023) 3–5× higher unreported

69,000+
Victims in Coinbase/TaskUs breach alone

784,000
Accenture employees with access to bank systems

THE DOCUMENTED CASE: COINBASE / TASKUS BREACH (2024–2025)

- A TaskUs contractor in Indore, India photographed and sold 200 customer records per day — names, SSNs, balances, government IDs — for $200 per image.
- Over 69,000 Coinbase customers were affected. Criminals impersonated Coinbase staff using the stolen data. Multiple victims lost their entire retirement savings.
- TaskUs concealed the breach for months, filed regulatory documents claiming no material breach, and simultaneously negotiated a $1.6 billion acquisition.
- Victims had no notification for 7 months — no law required it. No monitoring caught it. No whistleblower reported it safely.

EXAMPLE: Accenture — Truist Bank's primary outsourcing partner since 2017 — employs 784,000 people globally including 80,000 in Bonifacio Global City, Philippines, the same area where the U.S. Treasury has sanctioned scam compound operations. Truist forced laid-off employees to become Accenture contractors in 2024. Customers were never informed.

THE REGULATORY GAP

Current law does not require financial institutions or their contractors to:

- Disclose the geographic location of personnel with access to customer account systems
- Implement real-time behavioral monitoring at outsourced data access points
- Provide a protected reporting channel for overseas contractor employees

GLBA, OCC Third-Party Risk Guidance (2023-17), and Dodd-Frank all address adjacent issues — none close these specific gaps.

THREE TARGETED ASKS

1. Geographic Disclosure
Require banks to disclose in annual reports where third-party contractors with account access are located. (Amend GLBA §501)

2. Real-Time Monitoring
Mandate behavioral monitoring at all outsourced access points — key logging, anomaly detection, escalation protocols. (Joint OCC/CFPB rulemaking)

3. Whistleblower Pathway
Create a protected, anonymous reporting channel for outsourced contractor employees who observe data misuse. (Amend Dodd-Frank §922)

Sherry Spurlin | Spurlin Digital Solutions | Author: Digital Predators, HiJacked: The Digital Invasion, The Scammer's Playbook | @sherry_spurlin (TikTok, 25K+ followers)

Full policy brief with complete citations and documentation available on request.