POLICY BRIEF

Institutional Outsourcing and the Fraud Infrastructure Crisis:

How Third-Party Vendor Relationships Enable Financial Fraud Against Seniors and Vulnerable Americans

Prepared by Sherry Spurlin | Spurlin Digital Solutions | February 2026

EXECUTIVE SUMMARY

American financial institutions are quietly transferring core operational functions — including direct access to customer account systems, personal financial data, and transaction infrastructure — to third-party outsourcing contractors whose employees work in geographic regions with documented concentrations of organized fraud activity. This practice, executed under the banner of "digital transformation" and cost reduction, has created a structural vulnerability that no current federal regulation directly addresses.

The consequences are not theoretical. The 2024–2025 Coinbase/TaskUs data breach — in which a contracted employee in Indore, India systematically photographed and sold the personal financial records of over 69,000 customers — demonstrates the catastrophic human cost of unregulated outsourcing access. Victims, many of them seniors who had entrusted their retirement savings to these platforms, lost substantially all of their financial assets. The contracting company, TaskUs, allegedly concealed the breach while proceeding with a $1.6 billion acquisition, filing regulatory documents claiming no material breach had occurred.

This brief presents documented evidence of the outsourcing-to-fraud pipeline operating within major American financial institutions, identifies the specific regulatory gaps that allow it to persist, and proposes three targeted legislative and regulatory remedies that would protect seniors and vulnerable Americans without imposing unreasonable burden on the financial industry.

ASK	Congress should require financial institutions to disclose the geographic location of third-party contractors with access to customer account systems; mandate real-time monitoring at all outsourced access points; and establish a whistleblower pathway for outsourced employees reporting suspicious activity.

THE PROBLEM: THE OUTSOURCING-TO-FRAUD PIPELINE

How It Works

When an American opens a bank account, they reasonably believe their personal financial data — account numbers, Social Security numbers, transaction history, balances, government ID images — is being handled by employees of that institution, operating under its compliance and security frameworks. That assumption is increasingly false.

Major financial institutions have systematically transferred their customer service operations, IT infrastructure management, fraud investigation functions, and core banking platform support to third-party outsourcing giants. These contractors — among the largest being Accenture, TaskUs,

Teleperformance, Concentrix, Cognizant, and others — then staff these operations predominantly with employees in the Philippines, India, and other lower-wage markets.

The scale is difficult to overstate. Accenture alone employs 784,000 people globally, generates $69.67 billion in annual revenue, and has operated as the primary outsourcing partner for major institutions including Truist Bank since at least 2017. Accenture employees in this role do not merely answer phones. They manage IT infrastructure, run banking operations platforms, and have been described by internal employees as holding "root access" to core banking systems. Accenture operates approximately 80,000 employees in the Philippines alone — in Bonifacio Global City, the same geographic area where the U.S. Treasury has sanctioned scam compound operations.

KEY FACT	Truist Bank forced laid-off employees to become Accenture contractors in February 2024 or forfeit their severance, while routing 80% of operations offshore — without any public disclosure to customers whose accounts these contractors now accessed.

The Coinbase/TaskUs Breach: A Case Study in Regulatory Failure

The Coinbase/TaskUs breach provides the clearest documented illustration of where this systemic failure leads. Beginning in September 2024, Ashita Mishra, a TaskUs employee at the company's Indore, India office, began photographing up to 200 customer records per day and selling them for $200 per image to members of an organized cybercriminal network. The stolen data included names, email addresses, home addresses, bank account details, balances, and Social Security numbers belonging to over 69,000 Coinbase customers.

The criminal network used this data to impersonate Coinbase customer service representatives, contact victims by phone with verified personal details to establish trust, and manipulate them into transferring their cryptocurrency holdings. Some victims reportedly hired private security, fearing physical targeting due to the breach. Multiple victims lost substantially all of their retirement savings.

The institutional response was not containment — it was concealment. TaskUs fired 226 staff at its Indore office in January 2025. In February 2025, with full knowledge of the breach, TaskUs filed its Form 10-K declaring no awareness of any material breach — while simultaneously proceeding with negotiations for a $1.6 billion acquisition by Blackstone. The breach was not publicly disclosed until May 2025, when Coinbase received a $20 million ransom demand.

The victims, whose data had been compromised for seven months before any public disclosure, had no way to protect themselves during that window. No current federal law required TaskUs to disclose the breach promptly. No regulatory framework imposed real-time monitoring requirements on their employee access to customer financial data. No whistleblower pathway existed for the TaskUs employees who knew what was happening.

SCALE	FBI IC3 reported $3.4 billion in elder fraud losses in 2023 — the actual figure is estimated at three to five times higher due to chronic underreporting. Seniors over 60 reported the highest per-victim losses of any age group, averaging $33,915 per incident.

The Regulatory Gap

Existing regulatory frameworks were not designed for the current outsourcing landscape:

- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect customer data but does not require disclosure of which third-party contractors have access to that data, where those contractors operate, or what monitoring controls are in place at their facilities.
- The OCC's Third-Party Risk Management guidance (OCC 2023-17) provides a framework for banks to assess vendor risk, but compliance is assessed through internal bank processes — not through independent verification or public reporting. A bank can technically comply with OCC guidance while maintaining outsourcing arrangements that create the exact vulnerabilities this guidance was intended to prevent.
- No federal law currently requires financial institutions or their contractors to disclose the geographic location of personnel with access to customer account systems.
- No federal law establishes a secure, protected whistleblower channel specifically for outsourced contractor employees who become aware of data misuse or suspicious access activity.

The result is a system in which institutions bear no meaningful disclosure obligation, contractors face minimal monitoring requirements, and victims receive notification — if at all — only after their data has been actively exploited for months.

WHO IS BEING HARMED

The victims of this structural failure are not abstract. They are seniors who receive calls from individuals who already know their account balance, their recent transaction history, and their home address — because that information was purchased from a contracted bank employee for $200.

They are retirement-age Americans who spent decades accumulating savings and trusted regulated financial institutions to protect their data — not understanding that "regulated financial institution" now means an institution whose customer data is accessible to contractors operating in overseas facilities with inadequate monitoring and essentially no whistleblower protection.

This author is among them. I am a licensed mortgage professional with 30 years in financial services — trained to identify financial fraud, experienced in reviewing suspicious transactions — who was victimized beginning in October 2024 by individuals who demonstrated knowledge of my financial accounts consistent with insider access. My bank at the time, Truist, had outsourced core operations to Accenture. The pattern of information access in my case is consistent with what the Coinbase/TaskUs investigation subsequently documented on a mass scale.

If this could happen to a financial professional who knew what fraud looked like, it is happening to everyone who does not.

RECOMMENDATIONS

This brief requests three specific, targeted actions:

Recommendation 1: Mandatory Geographic Disclosure

Require financial institutions to disclose in their annual reports the geographic location of all third-party contractors and subcontractors who have access to customer account systems, personal financial data, or transaction infrastructure. This disclosure should be a material item in SEC filings and subject to the same accuracy requirements as other material disclosures. Customers should have the right to access this information on request.

Legislative vehicle:

Amendment to GLBA Section 501 (15 U.S.C. § 6801) or standalone elder fraud infrastructure transparency legislation.

Recommendation 2: Real-Time Monitoring Requirements at Outsourced Access Points

Direct the OCC and CFPB to issue joint guidance — with enforcement teeth — requiring financial institutions to implement and document real-time behavioral monitoring at all outsourced access points to customer data. This should include key logging software, anomaly detection triggers for bulk data access, and mandatory internal escalation protocols when suspicious access patterns are detected. The TaskUs breach involved an employee photographing 200 records per day over months. This should have triggered automated detection. It did not because no requirement existed.

Regulatory vehicle:

Joint OCC/CFPB rulemaking under existing third-party risk management authority, or congressional direction via Financial Services Committee oversight.

Recommendation 3: Outsourced Employee Whistleblower Pathway

Establish a federally protected, anonymous reporting channel specifically for outsourced contractor employees who become aware of data misuse, unauthorized access, or suspicious activity involving American consumer financial data. Current whistleblower protections do not clearly extend to foreign national contractor employees. This gap means that the employees most likely to observe insider fraud — low-wage overseas contractors — have no protected pathway to report it and significant personal risk if they attempt to do so informally.

Legislative vehicle:

Amendment to Dodd-Frank Section 922 whistleblower provisions or new elder fraud-specific legislation.

ABOUT THE AUTHOR

Sherry Spurlin is a licensed mortgage professional with more than 30 years of experience in financial services, including extensive work identifying fraudulent loan applications and suspicious financial activity. She is the founder of Spurlin Digital Solutions and Market 4 Social LLC, and the author of three published books on scam prevention: Digital Predators, HiJacked: The Digital Invasion, and The Scammer's Playbook. She maintains a fraud awareness platform with 28,000+ followers on TikTok (@sherry_spurlin) where she produces daily educational content reaching vulnerable Americans.

Her research into institutional enablement of fraud infrastructure is grounded in both professional expertise and personal experience as a documented victim of the outsourcing-enabled fraud pipeline she describes in this brief. She welcomes the opportunity to testify, brief staff, or provide supplemental documentation to any committee, agency, or investigative body engaged in protecting American consumers from financial fraud.

sherry@mortgagegroupllc.com

info@market4social.com

256-558-6199

Contact: Spurlin Digital Solutions | @sherry_spurlin (TikTok) | spurlindigitalsolutions.com

Books available: Digital Predators | HiJacked: The Digital Invasion | The Scammer's Playbook