GOVERNMENT BLOCKCHAIN ASSOCIATION, REMI ALLI

Proposal and Comment Information

Title: Proposed Third-Party Risk Management Guidance, OP-1881

Comment ID: FR-2026-0031-01-C43

Submitter Information

Organization Name: Government Blockchain Association

Organization Type: Organization

Name: Remi Alli

Submitted Date: 11/12/2026

Please find attached the formal interagency comment submission of Remi Alli, JD, MS, Chief Policy Adviser, Government Blockchain Association (GBA), regarding Proposed Interagency Third-Party Risk Management Guidance (91 Fed. Reg. 44445; Docket ID OCC-2026-0793 / Docket ID NCUA-2026-1684):

1. Formal Comment Letter: GBA Comment on Proposed Interagency Third-Party Risk Management Guidance
2. Exhibit A: Smart Friction: Designing Human-Centered Protection and Conflict Management in Digital Finance (GBA Policy White Paper Series No. 7694521 | ssrn.com)
3. Exhibit B: Chief Risk Officer (CRO) Audit & Constructive Notice Playbook (Mapped to Interagency Harm-Based Tailoring and Residual Risk Principles)

CHIEF RISK OFFICER (CRO) AUDIT & CONSTRUCTIVE NOTICE PLAYBOOK

Mitigating Third-Party Harm and Enforcing Legal Consent Under OCC Bulletin 2026-46 • Remi Alli, JD, MS (GBA Chief Policy Adviser)

Why Constructive Notice Is a Bank Risk Issue. Under traditional contract law, a user is bound by terms only when given **constructive notice**—meaning a reasonably prudent person could actually see, read, and understand material terms before committing capital. Prompting a retail customer to sign raw hexadecimal smart-contract code (`0x095ea7b3...`) or burying irreversible permissions inside forty-page clickwrap contracts represents a **collapse of constructive notice** (**Remi Alli, JD, MS**, *SSRN Working Paper Series No. 7694521*).

For sponsor banks and fiduciary institutions operating under **OCC Bulletin 2026-46** (Proposed Interagency Third-Party Risk Management Guidance), defective user consent is a direct **UDAAP** and litigation vulnerability creating material financial harm. To support documented **residual risk acceptance** within board risk appetite, digital asset partners must implement four auditable compensating controls:

1. Constructive Notice at the Point of Signature (Zero Blind Signing). Replace raw machine code with a four-part, plain-language summary prior to signature execution—explicitly stating the asset and dollar amount leaving custody, verified counterparty identity, whether the transaction is permanent, and total fees. Disclosures must strip out Wall Street and crypto insider jargon so everyday savers across diverse cultural communities understand exact risks (**Remi Alli, JD, MS**, *195: Business, Culture and Ethics Worldwide*).

2. Risk-Triggered Behavioral Pauses (Smart Friction). Keep routine transfers to verified contacts instant, while triggering a mandatory **thirty-second behavioral cooling-off window** and exact-amount permission caps whenever a user interacts with an unverified address or moves a large share of account holdings (**Richard Thaler and Cass Sunstein**, *Nudge*; **Remi Alli, JD, MS**, *SSRN Abstract No. 7694521*). Thirty seconds interrupts social engineering in real time and reduces unauthorized-transfer exposure.

3. Segregated Custody and Explicit Asset Boundaries. Maintain bankruptcy-remote one-to-one reserve segregation backed by live cryptographic attestations (**Dr. Christopher W. Smithmyer**, *The Stablecoin Book*) paired with verified, human-readable legal and intellectual property token metadata (**Remi Alli, JD, MS**, *Tokenize Everything*).

4. Contained Conflict Escalation (Zero-Cost Retail OCM). Embed a twenty-four-hour automated diagnostic check and a seventy-two-hour culturally neutral online mediation pathway at **zero retail filing cost** (**Dr. Christopher W. Smithmyer**, *The Mechanics Mediator*; **Remi Alli, JD, MS**, *SSRN Abstract No. 7694521*), backed by **Blockchain Maturity Model (BMM)** Level 3+ auditable state tracking and **Federal Rule of Evidence 702** assessor standards.

Remi Alli, JD, MS • Chief Policy Adviser, Government Blockchain Association (GBA)
remi@gbaglobal.org • gbaglobal.org • Citation: SSRN Abstract No. 7694521 (https://ssrn.com/abstract=7694521)

GOVERNMENT BLOCKCHAIN ASSOCIATION (GBA)

Office of the Chief Policy Adviser • Washington, D.C. • gbaglobal.org • Bridging law, technology and public trust.

November 16, 2026

Via Federal eRulemaking Portal (Regulations.gov)
Office of the Comptroller of the Currency (OCC)
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation (FDIC)
National Credit Union Administration (NCUA)

> **Re: Proposed Interagency Third-Party Risk Management Guidance — Docket ID OCC-2026-0793 / OCC Bulletin 2026-46 (91 Fed. Reg. 44445, Sept. 15, 2026)**

Dear Sir or Madam:

The Government Blockchain Association (GBA) appreciates the opportunity to comment on the Agencies' Proposed Interagency Third-Party Risk Management Guidance issued on September 11, 2026, and published in the Federal Register on September 15, 2026. As Chief Policy Adviser for the GBA, I submit these comments to support the Agencies' shift toward a tailored, principles-based framework and to offer four auditable compensating controls —drawn from behavioral choice architecture, contract law, cross-cultural ethics, and structured conflict management—that enable banking organizations to evaluate third-party digital finance relationships safely and document residual risk acceptance with confidence.

Replacing Rigid Category Labels With Harm-Based Tailoring

For the past three years, overly rigid application of the 2023 Interagency Guidance pushed many banking organizations into binary risk decisions. Too often, banks treated every fintech, payment processor, or distributed-ledger integration as an unmanageable "critical activity" regardless of actual consumer exposure. That all-or-nothing posture did not eliminate risk. It simply drove everyday savers and mission-driven founders away from supervised American banks and toward opaque, offshore platforms.

The Agencies' September 2026 proposal corrects that imbalance. By anchoring oversight in the **magnitude and likelihood of potential harm**—material financial loss, legal noncompliance, or severe operational disruption—and explicitly recognizing **formal residual risk acceptance** within a bank's stated risk appetite, the Agencies have created a workable supervisory path for responsible innovation. Yet principles-based guidance

succeeds in examination rooms only when Chief Risk Officers and second-line compliance teams possess concrete, measurable benchmarks to verify whether a third-party relationship actually contains harm.

Four Auditable Compensating Controls for Third-Party Digital Finance

To help banking organizations operationalize harm-based tailoring and document residual risk acceptance under the proposed guidance, the Agencies should recognize four testable compensating controls established in my policy white paper, *Smart Friction: Designing Human-Centered Protection and Conflict Management in Digital Finance* (**Remi Alli, JD, MS**, Government Blockchain Association Policy White Paper Series, SSRN Abstract No. 7694521).

1. Constructive Notice and Plain-Language Informed Consent. In traditional contract law, a consumer is bound only when given meaningful constructive notice of material terms. Prompting a retail banking customer to sign raw hexadecimal smart-contract code (`0x095ea7b3...`) or burying irreversible transfer permissions inside forty-page clickwrap contracts represents a collapse of constructive notice (**Remi Alli, JD, MS**, *SSRN Abstract No. 7694521*). Third-party interfaces integrated with banking organizations should translate every permission into plain everyday language prior to execution—specifying exact assets leaving custody, verified counterparty identity, permanence, and fees. Furthermore, consistent with cross-cultural business ethics standards examined in *195: Business, Culture and Ethics Worldwide* (**Remi Alli, JD, MS**), disclosures must eliminate Wall Street and technical insider jargon so diverse retail communities understand exact downside risks before committing funds.

2. Risk-Triggered Thirty-Second Behavioral Cooling-Off Pauses. Behavioral economists **Richard Thaler and Cass Sunstein** demonstrated in *Nudge* that frictionless choice environments invite predictable human error whenever people act under stress, distraction, or manufactured urgency. Modern social-engineering fraud rarely breaks cryptographic encryption; it exploits human panic during one-click execution. Banking organizations evaluating third-party payment or wallet providers should look for **Smart Friction** controls that keep routine, low-stakes transfers to verified recipients instant while triggering a mandatory **thirty-second behavioral cooling-off window** and exact-amount permission caps whenever a transaction involves a first-time external address or an unusually large share of liquid balances (**Remi Alli, JD, MS**, *SSRN Abstract No. 7694521*). Thirty seconds gives human judgment room to catch up with digital speed, measurably reducing unauthorized-transfer losses and UDAAP exposure.

3. Ring-Fenced Reserve Segregation and Explicit Asset Metadata. Front-end consent controls fail if underlying payment instruments carry hidden insolvency or legal ambiguity. Consistent with monetary reserve principles detailed in *The Stablecoin Book* (**Dr. Christopher W. Smithmyer**) and asset tokenization governance standards examined in *Tokenize Everything* (**Remi Alli, JD, MS**), third-party relationships involving payment stablecoins or tokenized assets should demonstrate bankruptcy-remote one-to-one reserve segregation backed by live cryptographic attestations, alongside permanent, human-readable metadata defining each asset's legal classification and intellectual property boundaries.

4. Contained Conflict Escalation Through Zero-Cost Retail Mediation. Third-party operational disruptions escalate into regulatory enforcement files when customers are abandoned to anonymous chat queues or unaffordable litigation. As **Dr. Christopher W. Smithmyer** demonstrates in *The Mechanics Mediator*, effective conflict resolution relies on structured behavioral de-escalation windows and neutral mediation before panic hardens into loss. Banking organizations should encourage third-party partners to embed a three-tier **Online Conflict Management (OCM)** funnel featuring twenty-four-hour automated diagnostics and a seventy-two-hour culturally neutral mediation pathway at **zero filing cost for retail participants** (**Remi Alli, JD, MS**, *SSRN Abstract No. 7694521*). Containing disputes inside a seventy-two-hour service-level window protects bank reputation, prevents chargeback spikes, and establishes quantifiable boundaries for residual risk acceptance.

Evidentiary Rigor in Third-Party Due Diligence and Ongoing Monitoring

Finally, as banks tailor due diligence and ongoing monitoring to the specific risk profile of each vendor, independent technical assessments must satisfy objective evidentiary standards rather than informal self-attestation. Under the GBA's **Blockchain Maturity Model (BMM)** evidentiary standards, formal infrastructure assessments are conducted by panels credentialed under **Federal Rule of Evidence 702 (*Daubert*)** benchmarks, governed by a strict twelve-month **ISO/IEC 17021** conflict-of-interest cooling-off firewall, backed by professional liability coverage, and anchored by senior **Full Expert gatekeepers** at initial intake. Recognizing objective, courtroom-grade maturity assessments within ongoing monitoring guidance allows banks—especially community and regional institutions—to verify third-party technical controls efficiently without duplicating costly engineering audits.

Conclusion

The Agencies' proposed principles-based guidance represents a vital step toward aligning bank third-party risk management with real-world harm prevention and responsible

innovation. By recognizing plain-language constructive notice, risk-triggered behavioral pauses, segregated reserve and asset metadata standards, zero-cost retail conflict escalation, and evidentiary maturity assessments as concrete compensating controls, the Agencies can empower banking organizations to onboard safe, transparent digital finance partners while protecting everyday consumers.

Respectfully submitted,

Remi Alli, JD, MS
Chief Policy Adviser
Government Blockchain Association (GBA)
remi@gbaglobal.org • gbaglobal.org
Bridging law, technology and public trust.

Attached Supporting Exhibit:
Remi Alli, JD, MS, *Smart Friction: Designing Human-Centered Protection and Conflict Management in Digital Finance*, Government Blockchain Association Policy White Paper Series No. 7694521 (Nov. 2026), https://ssrn.com/abstract=7694521.

GOVERNMENT BLOCKCHAIN ASSOCIATION (GBA) POLICY WHITE PAPER SERIES

Smart Friction: Designing Human-Centered Protection and Conflict Management in Digital Finance

Remi Alli, JD, MS
Chief Policy Adviser, Government Blockchain Association (GBA)

November 2026 | SSRN Working Paper Series No. 7694521 (https://ssrn.com/abstract=7694521)

Executive Summary

The central regulatory tension in modern digital finance is no longer whether open blockchain infrastructure will integrate with traditional banking—it is how everyday human beings can use self-custodial tools safely without surrendering autonomy to centralized gatekeepers.

Following the November 2026 midterm elections, federal banking agencies and incoming congressional committee leaders signaled an immediate shift toward strict retail consumer protection, third-party cyber accountability, and round-the-clock human customer support. Legacy financial institutions rely on **bad friction**—slow settlement delays, opaque holdbacks, and gatekeeping rules that exclude underbanked communities. Early Web3 interfaces overcorrected by eliminating *all* friction, turning irreversible blockchain transactions into one-click traps where a single spoofed link or unintelligible hexadecimal prompt can empty a family's savings in seconds.

Drawing on behavioral choice architecture, cross-cultural business ethics, monetary reserve standards, and online conflict management scholarship, this white paper establishes a middle regulatory standard: **Smart Friction**. Rather than banning self-custody or forcing decentralized wallets into legacy brokerage molds, smart friction deploys targeted, risk-triggered behavioral pauses, plain-language consent, verifiable asset boundaries, and zero-cost retail conflict resolution. The paper concludes with four testable safe-harbor benchmarks designed for legislative adoption, bank third-party risk supervision, and **Blockchain Maturity Model (BMM)** governance assessments.

1. The False Choice Between Wall Street Friction and Zero-Friction Traps

For decades, consumer financial protection relied on institutional friction. Wire transfers took days, cross-border remittances carried heavy intermediary fees, and compliance holds routinely froze accounts without explanation. While those barriers slowed certain types of fraud, they also imposed severe financial exclusion on working families and small businesses worldwide.

First-generation decentralized finance (DeFi) and self-custodial wallets promised the opposite: instant, borderless, peer-to-peer execution with zero intermediaries. Yet removing every pause from the user interface ignored a fundamental reality of human psychology. As behavioral economists Richard Thaler and Cass Sunstein

demonstrated in *Nudge*, frictionless choice environments invite predictable human error—especially when people make high-stakes decisions under stress, distraction, or manufactured urgency.

In digital asset wallets, zero-friction design created three systemic vulnerabilities:

- **Blind Smart-Contract Signing:** Retail users routinely sign raw hexadecimal code strings they cannot read, granting third-party applications unlimited access to drain wallet balances weeks or months later.
- **Real-Time Social Engineering:** Scammers rarely break modern cryptography; they exploit human panic. One-click execution leaves zero buffer for a user to spot a spoofed domain, a coerced transfer, or an address-poisoning attack before settlement becomes irreversible.
- **Abandonment After Failure:** When a software bug, oracle error, or commercial dispute occurs, users are frequently left with anonymous chat channels or unaffordable cross-border litigation—fueling the exact political backlash driving incoming 2027 congressional mandates for human customer support.

2. Defining "Smart Friction": Behavioral Design as Consumer Protection

Smart Friction treats interface delay as a precision safeguard rather than a blanket barrier. Routine, low-stakes transactions to verified contacts remain instant and seamless. High-risk anomalies automatically trigger calibrated pauses and plain-language disclosures that give human judgment time to catch up with digital speed.

A compliant Smart Friction architecture rests on three behavioral and legal pillars:

A. Abolition of Blind Signing & Constructive Notice

In contract law, valid consent requires meaningful notice of material terms. Forty-page clickwrap adhesion contracts and raw machine code fail that standard. Compliant interfaces must translate every smart-contract permission into blunt, everyday sentences prior to execution—specifying exactly what leaves the user's wallet, who receives spending authority, whether the action is reversible, and what fees apply. Furthermore, consistent with cross-cultural business ethics standards (*195: Business, Culture and Ethics Worldwide*, Remi Alli, JD, MS), disclosures must strip away Wall Street and crypto insider jargon so first-time savers across diverse global markets understand exact downside risks in their own cultural context.

B. Risk-Triggered 30-Second Behavioral Cooling-Off Windows

When an interface detects a high-risk anomaly—such as transferring funds to a brand-new external address, moving a large percentage of account holdings, or interacting with an unverified smart contract—it triggers a mandatory **30-second cooling-off pause**. During that window, the screen displays a concise social-engineering checklist (e.g., *"Are you being rushed by someone on a phone call or message?"*) and requires deliberate confirmation. Applying structured behavioral de-escalation principles (*The Mechanics Mediator*, Dr. Christopher W. Smithmyer) directly inside software interrupts scams in real time while preserving 100% user self-custody.

C. Bounded Permissions by Default

Smart-contract token approvals must default strictly to the exact transaction amount rather than unlimited wallet allowances. Users must also have a prominent, one-click permission dashboard to inspect and revoke active contract approvals without technical command-line knowledge.

3. Verifiable Asset Boundaries & Reserve Integrity

Behavioral interface protections fail if the underlying digital assets carry hidden insolvency or legal ambiguity. Consistent with monetary reserve principles (*The Stablecoin Book*, Dr. Christopher W. Smithmyer) and asset tokenization governance (*Tokenize Everything*, Remi Alli, JD, MS), compliant ecosystems must enforce two structural boundaries:

- **Ring-Fenced 1:1 Reserve Segregation:** Payment stablecoins and custodial balances must maintain strict legal segregation—backed 1:1 by cash or short-term sovereign liquidity held in bankruptcy-remote accounts so customer assets are never commingled with corporate operating funds.
- **Explicit Token & Intellectual Property Metadata:** Every digital asset supported within an institutional ecosystem must carry human-readable metadata declaring its exact legal classification, commercial scope, and underlying intellectual property rights—eliminating confusion between utility access, governance participation, and investment claims.

4. Pairing Prevention with Zero-Cost Online Conflict Management (OCM)

Even well-designed interfaces cannot prevent every operational glitch, merchant disagreement, or cross-border transaction dispute. To satisfy incoming legislative and banking expectations for human accountability without sacrificing digital efficiency, platforms should embed a three-tier **Online Conflict Management (OCM)** escalation ladder:

- **Tier 1 — Automated Diagnostics & Restitution (Hours 0–24):** Technical discrepancies, failed settlements, and verified interface errors are audited immediately against on-chain logs, with plain-language findings or automated restitution issued within 24 hours.
- **Tier 2 — Facilitated Negotiation & Neutral Online Mediation (Days 2–7):** Unresolved user, merchant, or protocol disputes enter a 72-hour guided negotiation window followed by culturally neutral online mediation—delivering fair, jargon-free settlements with **zero filing fees for retail participants**.
- **Tier 3 — Binding Expert Determination (Days 8–21):** Complex commercial, treasury, or technical disputes unresolved in mediation advance to an impartial three-member panel combining legal, technical, and cross-cultural expertise, issuing reasoned written determinations within 14 days.
- **Bounded Emergency Circuit Breakers:** Where escrow or bridge smart contracts incorporate emergency pause triggers to contain active cyber exploits, those triggers must be strictly time-bounded, governed by multi-signature oversight, and logged publicly on-chain.

5. Four Testable Safe-Harbor Benchmarks for Policymakers & Supervisors

Rather than relying on subjective assessments of "sufficient decentralization," lawmakers, federal bank examiners, and **Blockchain Maturity Model (BMM)** assessors can evaluate digital asset platforms against four objective, auditable benchmarks:

Safe-Harbor Benchmark	Auditable Requirement	Regulatory & Supervisory Benefit
1. Plain-Language Informed Consent	100% human-readable transaction translation; zero raw-hex blind signing; localized risk disclosures.	Establishes verifiable constructive notice and reduces deceptive-interface liability.
2. Risk-Triggered Cooling-Off Pauses	Mandatory 30-second verification delay and exact-amount permission caps on high-risk transfers.	Measurably reduces retail phishing losses without restricting self-custody.
3. 1:1 Reserve & Metadata Integrity	Bankruptcy-remote reserve segregation, cryptographic attestations, and explicit token/IP metadata.	Aligns with GENIUS Act reserve rules, bank third-party risk standards, and fiduciary safety.
4. Zero-Cost Retail Conflict Escalation	24-hour diagnostics, 72-hour negotiation, and zero-fee retail OCM backed by BMM Level 3 auditability.	Satisfies congressional human-support mandates and prevents disputes from escalating into enforcement files.

Conclusion

The next phase of digital finance adoption will happen on everyday mobile devices, not developer command lines. By pairing **Smart Friction** at the moment of decision with **verifiable asset boundaries** and **zero-cost Online Conflict Management** when disputes arise, policymakers and builders can protect everyday families without turning open digital networks into closed banking monopolies.

Remi Alli, JD, MS
Chief Policy Adviser
Government Blockchain Association (GBA)
remi@gbaglobal.org | gbaglobal.org
Bridging law, technology and public trust.

Suggested Citation: Remi Alli, JD, MS, *Smart Friction: Designing Human-Centered Protection and Conflict Management in Digital Finance*, Government Blockchain Association (GBA) Policy White Paper Series No. 7694521 (Nov. 2026), https://ssrn.com/abstract=7694521.