Payments as a Lifeline (PaaLPay.org)
[redacted]
https://www.paalpay.org

Sept 18, 2025

Submitted via Regulations.gov
RE: Comment Letter in Response to RFI: Docket ID OCC-2025-0009Docket No. OP-1866

Dear Honorable Leaders of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC),

This is Kim Hall, Founder of The K Factor and a member of the advisory board of PaaL. I support and implore you to strongly consider the content in this letter.

Payments as a Lifeline (PaaL) appreciates the opportunity to respond to the RFI on how your agencies could take actions collectively or independently in their varying respective roles to help consumers, businesses, and financial institutions mitigate check, automated clearing house (ACH), wire, and instant payments fraud.

PaaL is a 501(c)(3) coalition of the leading U.S. and global financial technology (fintech) companies focused on improving the speed, transparency, efficiency, and positive impact of aid and disaster-related payments to people and small businesses. PaaL members range from global giants with traditional payment rails, to smaller agile financial technology (fintech) companies - innovators in the US and globally - some using traditional payment rails, others focused on blockchain/distributed ledger, AI, and fintech payment methods.

In addition to its members, PaaL is grateful to have the PaaL Advisory Council comprised of some of the largest NGOS and non-profits in the humanitarian aid space like United Way, St Vincent DePaul, Boys & Girls Clubs, OperationHope, Global Empowerment Mission, more; Government (federal, state, local); corporate foundations; plus, local charities serving their communities on the front line every day.

PaaL's mission is to deliver funds to the right person, at the right time, for the right purpose – with data to prove it.

While this RFI broadly addresses payments fraud, PaaL's deep experience in time-sensitive disaster and aid settings offers valuable lessons for payments as they relate to the other often high fraud payment areas. PaaL members have consistently demonstrated fast, secure, scalable, and repeatable methods for delivering funds — including to un/underbanked Americans - while employing cutting-edge payments technology, identity verification and fraud prevention tools.

The section below addresses only the specific questions as related to disaster and aid payments. **Please see the summary at the end, for recommendations on what can be done NOW**. The goal is to drive disaster financial resilience (DFR) for people, small businesses, and communities across the US – reducing the structure damage and emotional scars that harm for generations. Through DFR, we leverage best in class fintech, blockchain, AI and other innovations that reduce waste, fraud, and abuse – and provide the immutable data to prove it.

We look forward to opportunities to drive progress, especially related to the urgent topic of disater, in coming weeks.

Questions 1-4 External Collaboration, as related to Disaster and Aid payments

1) Actions to increase collaboration among stakeholders to address payments fraud

- **Create a Disaster Payments Fraud Data Trust.** Stand up a neutral, industry governed, government advised utility that lets government, banks, fintechs, NGOs, and insurers share real-time fraud indicators, using privacy-preserving techniques.
- **Adopt a "common beneficiary identity graph" for disasters.** Consent-based matching that links aid applicant identities across programs (public and private sector grants), using privacy protecting tools like tokenization - to prevent duplicate or synthetic claims.
- **Identify pre-approved merchant & MCC controls for restricted-purpose aid.** Shared merchant whitelists/blacklists and MCC/time/geo controls for e-cards and accounts to assure funds are delivered to the right person, at the right time, for the right purpose.
- **Create standardized incident codes & data fields.** Common fields for claim, identity, and fraud typologies (e.g., ISO 20022-style extensions) to make cross-entity analytics possible in near-real time.
- **Stand up red-team exercises for disaster scenarios.** Regular simulations (pre-season for hurricanes, floods, wildfires) that include banks, fintechs processors, wallets, state agencies, NGOs, foundations, more - and mobile OS/telco partners to test controls against current mule/SIM-swap/account-takeover patterns.
- **Create regulatory safe harbors for high-velocity sharing.** Clarify that good-faith real-time sharing of fraud indicators and beneficiary-risk scores among vetted members is permitted (and encouraged) when disasters are declared – before, during and after the disaster for aid purposes

2) Most effective collaboration types (incl. standard-setting) & the biggest obstacles

- **Interoperable technical standards**
  - **Identity:** NIST 800-63 IAL2/AAL2 alignment; FIDO2/WebAuthn passkeys for beneficiary/agent login; optional W3C Verifiable Credentials for "Aid-Eligible" proofs that are portable across programs.
  - **Messaging & data:** ISO 20022 extensions for disaster-aid disbursement, merchant-control flags, and fraud outcomes; standard payloads for device reputation and mule risk.
  - **Controls:** Common schemas for MCC/merchant whitelists, geofences, spend caps, cooling-off periods, and exception workflows.
- **Operational MOUs and joint SOC playbooks.** Shared escalation paths (who blocks, who reverses, who investigates), 24/7 contacts, and SLAs during declared emergencies.
- **Data-clean-room collaboration.** Compute-to-data models so banks, state agencies, NGOs and other disaster response and funding teams, learn from pooled data without moving or exposing PII.

Biggest obstacles

- **Legal/privacy silos & uncertainty.** Fragmented federal/state privacy rules and program statutes inhibit timely sharing; ambiguity around what can be shared in "near-real-time."
- **Data quality & identity fragmentation.** Inconsistent capture of identity attributes and addresses during crisis intake; lack of standardized evidence tiers.
- **Procurement & funding friction.** States/NGOs lack budget or authority to join shared utilities quickly.
- **Uneven technical maturity.** Small issuers, local agencies, and smaller NGOs often can't implement strong auth, device signals, or API standards without help.

- **Incentive misalignment.** Liability and recovery benefits don't always accrue to the party bearing the control costs.

3) Non-payments/banking organizations that should be collaborators

- **Disaster response & relief:** federal and state emergency management; leading NGOs (e.g., United Way, Global Empowerment Mission), VOAD networks; public adjuster associations; insurers/TPAs (for claim verification signals).
- **Identity & address signal providers:** SSA (death master file checks); USPS (address validation & change-of-address intelligence); state DMVs; utility companies and major landlords/property data providers (residency evidence).
- **Telecom & mobile ecosystem:** Major carriers (SIM-swap/port-out alerts), Apple/Google (device integrity, passkey adoption), MNO-based location verification for geo-locked benefits.
- **Cyber/fraud intel communities:** federal and state cyber fusion centers, and academic/industry anti-fraud labs for typology research and open datasets.
- **Social & commerce platforms:** To flag organized recruitment of mules and disaster-scam content; enable rapid takedowns during declared events.
- **Civil society & accessibility groups:** To ensure controls don't block vulnerable or unbanked populations (e.g., tribal communities, undocumented survivors, people without smartphones).

4) How increased collaboration among Federal & State agencies could help (and how to do it)

- **Stand up a one-Stop "aid identity gateway."** Created and run by industry collaborators, federally supported but state-integrated gateway that:
  - Performs **consistent risk-based identity proofing**
  - Issues a **portable verifiable credential** ("aid-eligible") that other programs/issuers can trust, and
  - Exposes **standard APIs** for eligibility checks, duplicate-claim detection, and fraud-risk scores.
- **Real-time Fraud Signal Exchange.** A joint Fed-State feed that distributes:
  - Confirmed mule accounts/beneficiaries, device fingerprints, SIM-swap events, merchant-collusion alerts, and synthetic-ID patterns;
  - Outcome labels (chargeback reason codes, clawbacks, recoveries) to continuously improve upstream screening.
- **Pre-approved Controls Library.** Best practices industry created federal guidance that states can "adopt by reference": MCC whitelists, permissible geo/time locks, exception relief rules, and minimum authentication standards for disbursement instruments.
- **SAR/314(b)-like safe harbor for disaster periods.** Time-bound safe harbor that explicitly permits cross-program sharing of fraud indicators and model outputs when a federal disaster is declared.
- **Joint recovery & clawback playbooks.** Standard processes for freezing/reversing funds across issuers/processors; coordinated referrals; measured timelines to minimize false positives.
- **Equity & access guardrails.** Nation level monitoring for disparate impact; mandated manual fallback paths (in-person proofing, call-center overrides), multilingual support, and device-loaner or OTP-by-voice options for the unconnected.

Questions 5-8 Consumer, Business, and Industry Education, as related to Disaster and Aid payments

5) Most effective types of payments-fraud education (by audience)

Cross-cutting principles (why they work in disasters):

- **Just-in-time + embedded**: put the right warning at the exact moment of risk (during application, disbursement, or first spend) rather than generic PSAs.
- **Concrete scripts > abstractions**: tell people *exactly* what to do/say (e.g., "Hang up. Call relief at ###," "Banks will never ask for your one-time code").
- **Scenario training**: show real scam flows (imposter calls, SIM-swap, mule recruitment, fake donation links) using screenshots/UI mockups.
- **Multichannel + low-tech**: SMS/IVR, radio, flyers at shelters, and faith/community centers—because many survivors have limited data or devices. In disaster the true residents turn to long standing trusted institutions – like faith and community centers. These are powerful organizations in disaster response/relief as they already know these residents. The fraudsters usually avoid these places as know they'll be called out as NOT belonging fast.

Consumers / survivors:

- **Micro-modules** in claims/disbursement portals (30–60 seconds): "3 red flags," "what to do if you clicked," "how your card is restricted-use."
- **Transaction-aware nudges**: in-app banners or SMS when spend attempts are declined for MCC/geo reasons, explaining *why* and how to get exceptions.
- **Plain-language checklists**: "Never share codes," "Refunds only to your original card," "Where to verify outreach."
- **Language & accessibility**: top local languages; 6th-grade reading level; ADA/Section 508 compliant; phone-tree equivalents.

Small businesses / merchants serving survivors:

- **Countertop one-pagers & POS prompts**: how restricted-use cards work, common fraud patterns, refund rules, and escalation contacts.
- **Short POS-provider webinars** (recorded) before/after major events; chargeback **playbooks** for aid instruments.

Industry (banks, fintechs, NGOs, agencies):

- **Live tabletop drills** before peak seasons; role-based runbooks for call centers, risk ops, and social teams.
- **Copy libraries** for consistent transaction-warning language across issuers and wallets; standards/best practices adoption guides to reduce spoofing.
- **Mule-risk education** for frontline staff and community partners (how recruitment appears on social/messaging apps; how to report).

6) Would more consumer/business education help reduce fraud and promote safe access?

Yes—if it is targeted, embedded, and measured.

- **Targeted** to local languages, scam typologies, and the instrument actually used (prepaid/e-card, wallet, ACH).
- **Embedded** at the moment of action (application intake, KYC step-up, first login, first spend, refund/chargeback).
- **Measured** with clear KPIs: reduction in ATO attempts, SIM-swap losses, duplicate-claim rate, % of users who complete a micro-module before first spend, time-to-report after exposure.

Education should increase access, not scare people away. Framing must emphasize protections ("your card only works at essentials; here's how to get exceptions for medical needs") and provide human fallbacks (walk-in verification, call-center scripts, assisted device/passkey setup).

7) Approaches to make existing fraud education more effective

- **Place education inside the flow**:
  - To engage the REAL survivors and weed out the fraudsters, leverage the long standing trusted community and faith based organizations as sites for intake, access to technology, and a general safe space in the chaos
  - Application portals: a 45-second anti-imposter module before submitting.
  - Disbursement screens: explain restricted-use controls (MCC, geo, time) and refund rules.
  - First transaction: short message "don't share codes; issuer will *never* ask" with a single "I understand" tap.
- **Standardize and syndicate**: a federal/state copy kit (plain text + iconography) and API that issuers, wallets, NGOs, and states can pull into apps, SMS, IVR, and web—kept current during an active disaster.
- **Localize and narrowcast**: geo-target push/SMS/radio when a disaster is declared; rotate messages based on the dominant fraud typology (e.g., "FEMA imposter calls reported in your county").
- **Co-brand with trusted senders**: federal and state Emergency Management Agencies + fintech bank/wallet + known NGO; use verified sender marks to reduce spoofing risk.
- **Partner channels**: shelters, schools, tribal offices, utility bill inserts, pharmacy counters; two-sided education(consumers and merchants) to reduce confusion at checkout.
- **Behavioral design**: pre-commitment prompts ("If someone asks for your code, what will you do?"), loss-aversion framing, and safe defaults (passkeys, auto-enabled alerts).
- **Continuous A/B testing**: iterate message length, order, and tone; publish what works in a shared dashboard.
- **After-action loops**: feed confirmed fraud patterns back into the education content within 24–72 hours.

8) Are current online resources effective? How to improve

Gaps we observe in disasters:

- Fragmented across fed/state agencies, NGOs, foundations, nonprofits - hard to find the single source of truth.
- Web-first, text-heavy, English-only; rarely optimized for low bandwidth or older devices.
- Few concrete screenshots of *actual* scam patterns; limited guidance for restricted-use cards and exception workflows.
- Static pages; slow updates when fraud typologies shift.

Improvements we recommend:

- **Create a canonical "Disaster Payments Safety Hub"** with:
  - **Plain-language playbooks** for survivors, merchants, and helpers;
  - **Interactive scenario walk-throughs** (ATO, SIM-swap, imposter, mule recruitment, fake charities), with screenshots and scripts;
  - **Low-bandwidth mode** (no images by default), printable one-pagers, etc.
  - Live status panel: known scams in the current disaster, verified contact numbers, how to check a case;

  - **Exception request explainer** for restricted-use cards (medical devices, temporary lodging, mobility aids);
  - **Accessibility & language coverage** aligned to local demographics.
- **Syndication toolkit**: SMS templates, 30-second audio spots for transportation hubs (bus and train stations, airports, etc.), radio, social assets, and QR codes (with warnings about QR phishing).
- **Verification cues**: guidance for short .gov and .org URLs, and "verify-before-you-click" steps.
- **Metrics & transparency**: publish engagement and impact (module completion can drive loss reduction), and retire underperforming content.

Questions 9-15: Regulation and Supervision

We defer to other experts in this space and are not commenting on this section

Questions 16-20: Payments Fraud Data Collection and Information Sharing as related to Disaster and Aid payments

16) How to improve payments-fraud data collection & information sharing

- **Define a common disaster-payments fraud schema.** Publish a minimal, interoperable dataset (attempts + outcomes). Potentially make it extendable from ISO 20022/FraudClassifier℠: identity-proofing tier, instrument type (prepaid/wallet/ACH), MCC controls applied, geo/time locks, exception flags, device integrity, SIM-swap/port-out signal, duplicate-claim indicator, recovery status.
- **Shift from case-based to event-level telemetry.** Collect standardized *attempt* data (failed proofing, OTP replay, denied MCC spends) alongside confirmed fraud to surface precursors quickly.
- **Outcome labels and feedback loops.** Require consistent disposition codes (confirmed/suspected, typology, recovery/clawback) so models and education content improve within 24–72 hours.
- **Federated sharing with privacy-preserving record linkage (PPRL).** Use top tools to match beneficiaries, devices, and mule accounts across agencies/issuers without centralizing raw PII.
- **Time-bounded "disaster mode."** When a federal disaster is declared, enable near-real-time indicator exchange (mule accounts, device clusters, merchant collusion) with clear start/stop dates and minimization rules.
- **Quality & governance.** Create data quality SLAs (e.g., freshness, completeness, false-positive rate), an appeals process, and audit trails to protect consumers and small merchants.

17) Barriers to collecting/sharing data & how to alleviate them

Key barriers

- **Legal ambiguity/privacy silos.** Unclear authority to share cross-program fraud indicators in near real time; 314(b) is AML-focused, not disaster fraud.
- **Contractual & procurement friction.** States/NGOs/non-profits lack standard terms to join shared utilities quickly.
- **Inconsistent schemas & identity fragmentation.** Intake forms, evidence tiers, and addresses vary widely across programs.
- **Data sensitivity & liability fears.** Concern about mislabeling beneficiaries/merchants; lack of redress mechanisms.

- **Uneven technical maturity.** Smaller issuers, NGOs, and local agencies cannot implement APIs, passkeys, or PPRL without help.

Alleviations

- **Issue a disaster-fraud safe harbor.** Time-bounded protection for good-faith, minimal, standardized sharing of indicators and risk scores among vetted participants.
- **Model contracts & MOUs.** Publish plug-and-play terms (privacy, retention, redress, audit) for states, NGOs, issuers, and processors.
- **Regulator-profiled standards.** Provide "Disaster Payments Profiles" for ISO 20022 + Fraud/ScamClassifier extensions and a reference API.
- **Privacy-by-design tooling.** Fund clean-room/PPRL utilities and open-source SDKs for smaller participants.
- **Governance & redress.** Require transparent scoring documentation, human review pathways, rapid correction of bad labels, and equity monitoring.

18) Role for the FRS, FDIC, OCC (incl. FraudClassifier℠ / ScamClassifier℠)

- **Convene & codify.** Lead a multi-stakeholder working group to publish a **Disaster Payments Fraud Profile** (data fields, typologies, event/outcome codes, timeliness SLAs).
- **Extend classifiers for disaster context.** Add codes for: duplicate-claim attempts, restricted-use (MCC/geo/time) circumvention, merchant collusion at essentials, charity-fraud overlays, SIM-swap timing relative to disbursement, and exception-abuse.
- **Reference implementation & sandbox.** Sponsor an open reference API (event intake, indicator exchange, outcome feedback) and a supervised pilot using PETs (clean rooms/PSI).
- **Safe harbor & supervisory clarity.** Jointly issue guidance on time-bounded sharing during declared disasters, acceptable PETs, data minimization, retention, and consumer redress.
- **Data quality & fairness guardrails.** Require model cards/scorecards, bias testing across protected classes, and auditable explainability for adverse actions (holds/denials).
- **Certification & attestation.** Create a light-touch attestation for participants implementing the Profile (akin to SOC-type reporting for controls).

19) High-impact data types & who should collect/share them

- **Attempt-level authentication signals** (failed proofing tiers, OTP replay, device integrity attestation, IP/ASN anomalies); *Issuers, processors, wallet providers.*
- **Telecom events** (SIM-swap/port-out within ±7 days of disbursement; risky call-forwarding changes); *MNOs via gated feeds.*
- **Mule-account network indicators** (first-use velocity, P2P fan-out, shared device/IMEI clusters, repeat refund abuse); *Banks/fintechs/processors, aggregated via ISAO/clean room.*
- **Restricted-use control telemetry** (declined MCC/geo/time attempts, exception approvals); *Issuers/program managers.*
- **Merchant-level outcomes** (collusion flags, refund behavior, chargeback reasons, terminal reprogramming anomalies) with standard merchant IDs ; *Acquirers/processors.*
- **Duplicate-claim linkage tokens** (pseudonymous cross-program dedupe) and eligibility verification events; *Federal/state agencies + NGOs* using PPRL.
- **Recovery/clawback outcomes** (amount recovered, days to recover); *All participants* to close the loop.

  If not currently collected, regulators should designate responsible collectors above and route sharing through an industry created, governed trusted ISAO/Data Trust.

20) Centralized repositories—need, risks, and who should build them

Do we need one?

- For disaster payments, a federated model is preferable: keep raw PII with the source; share indicators, pseudonymous link tokens, and query results via clean rooms/PPRL. This reduces breach and mission-creep risk while enabling fast detection.
- If any centralization is used, limit it to indexes/metadata and outcome labels, not full identity datasets.

Risks & challenges

- **Privacy & breach concentration** (single honeypot).
- **Mislabeling & due-process** risk (hard to correct at scale).
- **Mission creep** beyond disaster scope; **equity impacts** if models learn from skewed data.
- **Inconsistent legal regimes** (state privacy laws, program statutes).
- **Operational single point of failure** during crises.

Mitigations

- **Federated architecture** with PETs; strong minimization and retention limits.
- **Independent governance** (public-interest charter, multi-stakeholder board, civil-rights oversight).
- **Appeals & correction SLAs** for beneficiaries and merchants.
- **Transparent documentation** (model cards, data dictionaries, change logs).
- **Time-bounded "disaster mode."**

Who should develop/participate

- **Lead/govern:** A neutral, non-profit Disaster Payments industry created and run trusted data platform, chartered with public-interest obligations, informed by existing regulator-endorsed rules of the road.
- **Participants:** Federal/state agencies, banks/issuers, processors, fintechs, blockchain and AI providers, acquirers, non-profits, major platforms, NGOs, insurers/TPAs.
- **Regulators' role:** Gain insights from FRS/FDIC/OCC to help set the Profile, safe harbor, and oversight; leverage CISA/FTC expertise for security/consumer protection collaboration.

Questions 21-22: Reserve Banks' Operator Tools and Services

We defer to other experts in this space and are not commenting on this section

Questions 23-26 General Questions, as related to Disaster and Aid payments

23) Most impactful fraud types & tactics we observe in disaster/aid payments

Fraud types (ranked by impact in our disaster ecosystem):

- **Imposter scams targeting survivors** (posing as FEMA/state/NGO/bank) to harvest OTPs, credentials, and card numbers.
- **Account takeovers (ATO) & social-engineering-assisted ATO** (SIM-swap/port-out within days of disbursement; OTP relay; MFA fatigue).
- **Synthetic and manipulated identities** at application/intake; **duplicate claims** across programs via slight data variations.
- **Mule account networks** used to cash-out e-benefits or launder restricted-use funds through collusive merchants.
- **Merchant collusion and refund abuse** (e.g., fake essential purchases, off-MCC goods, cash-like refunds to different instruments).
- **Charity/relief donation fraud** (fake links/QRs; spoofed domains; social platform recruiting).
- **Phishing via low-bandwidth channels** (SMS/WhatsApp/voice IVR) that mirror real agency scripts during outages.

Common tactics:

- **Real-time OTP interception** (live call handoffs, "helpdesk" scripts, man-in-the-middle pages).
- **SIM-swap + rapid credential reset** timed to funding windows.
- **Bypassing restricted-use controls** via collusive merchants, manipulated MCCs, or high-risk refund flows.
- **Geo-spoofing & device emulation** to fake presence in declared disaster zones.
- **Coordinated duplicate-claim patterns** (shared addresses/phones/devices across applicants) and **first-use velocity spikes** across new accounts.

24) Measures most effective for identifying, preventing, and mitigating fraud (and what consumers can do)

Controls that work in practice (PaaL coalition experience):

- **Strong authentication by default:** FIDO2/WebAuthn passkeys with device binding; phishing-resistant step-up for high-risk actions (add payee, change phone, first disbursement, exception requests).
- **Telecom risk integration:** carrier SIM-swap/port-out events and risky call-forwarding flags gating disbursement and credential resets.
- **Restricted-use instrumentation:** MCC/merchant whitelists, geo/time fences, spend caps, cooling-off periods; transparent exception workflows with auditable trails.
- **Event-level telemetry + real-time rules:** failed proofing, OTP replay, device integrity attestation, first-use velocity, refund anomalies; auto-quarantine + human review for multi-signal hits.
- **Merchant-side defenses:** acquirer monitoring for MCC drift, abnormal refund ratios, terminal reprogramming, and cross-merchant device/IMEI reuse.
- **Privacy-preserving indicator sharing:** federated clean-room/PPRL to exchange mule accounts, device clusters, duplicate-claim tokens, and outcomes.
- **Consistent survivor education in-flow:** 45-second micro-modules at application, first login, and first spend; standardized "issuer will never ask for your one-time code" prompts; clear decline explanations.

Helpful consumer actions (we actively encourage):

- **Enroll passkeys** and keep a SIM PIN; avoid SMS as the default factor when passkeys are available.
- **Nominate a trusted device/number** at intake; report number changes immediately.

- **Use official portals/links** (.gov or verified NGO/issuer) and never share OTPs—even with callers claiming to be from FEMA or a bank.
- **Request exceptions only through in-app/official channels** (not via links sent over SMS/DM), and with in-person interactions with long time trusted civic and faith based organizations.
- **Report suspected fraud within minutes** (in-app "Report fraud" + hotline) and freeze the instrument if compromised.

25) Additional actions to support stakeholders in detection, prevention, and mitigation

- **"Disaster Mode" guidance + safe harbor:** time-bounded permission for near-real-time sharing of indicators and risk scores among vetted members using PETs; standardized retention/minimization.
- **Disaster Payments Fraud Profile (standards):** industry created, regulator-endorsed data fields/typologies (attempts + outcomes), outcome labels, timeliness SLAs, and a reference API.
- **Exception governance kit:** model policies for medical/lodging exceptions, required evidence tiers, turnaround SLAs, and equity safeguards to avoid wrongful denials.
- **Merchant engagement package:** countertop explainers, refund scripts, acquirer alerting, and fast off-boarding for colluders—balanced with appeal paths for small merchants.
- **Red-team exercises pre-season:** cross-sector simulations (banks/fintechs/NGOs/states/MNOs/platforms) to test SIM-swap, OTP relay, duplicate-claim, and merchant-collusion scenarios.
- **Outcome transparency:** publish anonymized metrics (attempts blocked, false-positive rates, recovery/clawback times, education uptake) to drive continuous improvement and accountability.
- **Accessibility & civil-rights guardrails:** required manual fallback (in-person proofing, call-center overrides), multilingual content, and measurement for disparate impacts.

26) Actions to encourage use of payment methods with strong security features

- **Set minimum assurance baselines for aid rails:** require phishing-resistant auth (passkeys) and device integrity attestation for survivor and agent portals; AAL2 for high-risk actions.
- **Prefer tokenized, device-bound instruments:** push-provision cards to mobile wallets with device attestation; default to dynamic CVV/tokenization over PAN-entry.
- **Align incentives:** reduced dispute windows/fees and faster exception approvals for programs that meet security baselines; procurement points or grant preference for compliant issuers and NGOs.
- **Verified sender requirements:** DMARC/BIMI/VMC for all government/issuer/NGO communications; short, memorable verified URLs/handles.
- **Consumer-visible safety cues:** simple "Secure by Design" badging for aid instruments that meet the baseline (passkeys + tokenization + restricted-use controls).
- **One-tap security enrollment:** make passkey setup and alerts opt-out (not opt-in) at first login; provide assisted setup in shelters/community centers.
- **Merchant acceptance standards:** acquirers flag essential-category merchants with updated MCC controls and require anti-refund-abuse safeguards for participation in aid programs.

Summary and impact: PaaL (Payments as a Lifeline) — Commitments, Pilots, and Support for Regulators & Stakeholders

PaaLPay.org is a 501(c)(3) coalition of leading fintech, payments, blockchain, and AI firms focused on delivering disaster and aid funds to "right person, right time, right purpose—with the data to prove it." To operationalize the recommendations in this comment (focused on disaster and aid payments), PaaL looks forward to the opportunity to discuss and collaborate on how PaaL and its fintech/blockchain/AI members can drive key public and private sector orgs/leaders to deliver the following:

1) Standards, Reference Designs, and Tooling

- Disaster Payments Fraud Profile (open spec): Event/outcome fields, JSON schemas, typologies (incl. duplicate-claim, SIM-swap timing, MCC/geo/time circumvention), timeliness SLAs, and outcome labels.
- Reference Architecture: End-to-end blueprint for aid rails (passkeys + device attestation, telecom-risk, restricted-use controls, exception governance, PETs-based sharing).
- Open Taxonomies & Control Libraries: MCC whitelists/blacklists, geo/time fences, spend caps, exception evidence tiers, and refund/chargeback reason mappings.
- Copy & UI Kits: Plain-language, co-brandable content and screens for survivor onboarding, first spend, exception requests, decline explanations, and refund flows.

2) Privacy-Preserving Data Collaboration

- Disaster Payments Fraud data trust (pilot): Industry driven, neutral governance, privacy-preserving record linkage (clean rooms/TEEs/PSI), standardized indicator exchange (mule accounts, device clusters, merchant-collusion signals), and outcome feedback loops.
- PPRL SDKs and Templates: Implementation guides and open-source components to help smaller agencies/NGOs/issuers participate without centralizing raw PII.

3) Identity & Eligibility Enablement

- Aid Identity Gateway (reference design): Risk-based proofing aligned to NIST 800-63 (IAL2/AAL2), phishing-resistant authentication (FIDO2/WebAuthn), and optional verifiable credentials for portable "aid-eligible" attestations and cross-program duplicate-claim prevention.

4) Education & Outreach at Scale – consumers, small businesses, communities

- Have in advance, relationships with the local long time trusted entities – civic, faith based – who can engage their communities before, during, and after. These leaders have the trust of the community to get them to engage early and act quickly.
- Craft survivor, Community leaders & Merchant Education Kits: Embeddable micro-modules (web/app/SMS/IVR), printable one-pagers, radio scripts, and POS countertop materials explaining restricted-use cards, refund rules, and common scams.
- Be prepared with syndication & Narrowcast: API/JSON feeds and localized SMS/radio assets to rotate messages by county and fraud typology during active disasters.
- Executive continuous A/B Testing: Coalition-wide experiments with anonymized reporting on message effectiveness and behavioral outcomes.

5) Exercises, Governance, and Equity Safeguards

- Seasonal Cross-Sector Red-Team Drills: Joint simulations (banks/fintechs/NGOs/states/counties/cities, non-profits, platforms) for OTP relay, SIM-swap, duplicate-claim, and merchant-collusion scenarios; publish anonymized findings.
- Exception Governance Kit: Craft, test and execute model policies for medical/lodging exceptions, turnaround SLAs, audit trails, and equity monitoring; appeal and human-review pathways.
- Transparency & Metrics: Anonymized dashboards (attempts blocked, false-positive rates, time-to-recover, education completion) to support continuous improvement.

6) Implementation Support & Attestations

- Sandbox & Reference APIs: Test environments for event intake, indicator exchange, and outcomes publishing—aligned to the Disaster Payments Fraud Profile.
- Attestation Support: Templates/checklists for programs and providers to self-attest to baseline controls (e.g., passkeys, device attestation, DMARC/BIMI/VMC, restricted-use standards).
- Merchant Engagement Pack: Acquirer alerts, onboarding/off-boarding playbooks, refund-abuse safeguards, and balanced appeal processes for small merchants.

Availability: PaaL can drive a collaboration of needed parties – a small group of select federal/state/local agencies, NGOs, non-profits, civic/faith based orgs, and the PaaL financial services organizations – to establish readiness and pilots in blue sky. This proven readiness of a small group can build a playbook to be shared with other interested and engaged regions/communities. Together we can drive disaster financial resilience for all perils, making people, small businesses, and communities more resilient and with lower short and long term impacts of disasters.

The PaaL Members (fintechs, blockchain, AI, payments companies) and Advisory Council (largest NGOs, foundations, corporates, fed/state/local government, insurers, banks) stand ready to support your agencies, industry, NGOs/non-profits, in using advanced tools and collaborations to reduce fraud. Our expertise and mission is to especially focus on disaster and aid – delivering funds to the right person, right time, right purpose -with the data to prove it.

Sincerely,

[redacted]

Kim Hall
Founder, The K Factor

P.S. PaaL also hereby references support of the comment letter filed by the Faster Payments Council as well