JACOB ENGBERSON

Proposal and Comment Information

Title: Proposed Revisions to the Federal Reserve Policy on Payment System Risk and the Guidelines for Account and Services Requests, OP-1878

Comment ID: FR-2026-0013-01-C29

Submitter Information

Name: Jacob Engberson

Submitted Date: 07/17/2026

see comment in docx

Docket No. OP-1878

The proposed Payment Account framework asks how the Federal Reserve System can expand direct payment access while protecting settlement integrity, operational stability, and the financial system from illicit-finance risk. Those objectives depend upon the accuracy of the information, triggers, institutional decisions, and corrective processes operating within the framework.

A Payment Account determination develops through a connected chain:

Legal authority → governing program or rule → source data → screening engine → alert → assigned reviewer → institutional disposition → downstream consequences.

Each stage adds meaning to the stage before it. Source data becomes a trigger through a screening rule. The trigger becomes a classification through institutional interpretation. The classification becomes a consequence through human or automated action. That consequence may then produce additional activity that the system treats as new evidence of risk.

The integrity of the final determination therefore depends upon the integrity of the complete chain.

The Board’s immediate concern involves access, settlement, liquidity, and risk. This comment addresses those concerns at their point of origin. Effective risk management begins by identifying the actual exposure, preserving the trigger’s genesis, examining institutional causation, assigning responsibility to the actor or system that created the condition, and matching the response to the validated risk.

That examination must extend in both directions. It must follow the trigger backward to the event, source data, governing rule, institutional conduct, and prior notices that gave the event meaning. It must also follow the trigger forward through every restriction, affiliated system, intermediary, derivative alert, and downstream record affected by the classification.

Notice provides the first test of reciprocal accountability. Financial institutions require smaller participants to submit complete information, answer inquiries, meet deadlines, and correct deficiencies. A legitimate framework requires the institution exercising adverse authority to honor the same standard. When an applicant, member, or affected party gives timely notice, the institution should acknowledge it, investigate it, preserve it within the decision record, and answer it before an adverse conclusion becomes final or spreads through connected systems.

Risk must also receive complete accounting. A control may reduce risk, retain it, distribute it, or transfer it. Moving exposure outside one institutional boundary does not establish that the payment system became safer. The Board should examine where the risk traveled, who received it, whether that

participant could carry it, and whether the transfer created greater concentration, opacity, delay, or operational dependency elsewhere.

The four addenda develop that inquiry in sequence:

Trigger: What caused the system to react, and who controlled each stage of the classification?

Mitigation: Did the proposed control reduce the actual risk or merely transfer it to another institution, intermediary, or community?

Genesis: Did the decision record include the transaction, prior notices, institutional conduct, and source information existing before the trigger?

Reciprocity: Did the institution honor the same duties of notice, disclosure, correction, and accountability that it imposed upon the affected participant?

These questions support a practical framework. Each material determination should identify the originating data, governing authority, screening rule, trigger category, reviewer, evidence considered, prior notices, institutional contribution, final disposition, correction procedure, and every downstream recipient of the resulting classification.

A reliable Payment Account system measures risk with the same discipline used to measure assets and liabilities. It preserves the complete ledger of causation. It records the conduct of the applicant and the conduct of the institution. It distinguishes an observed event from the meaning later assigned to it. It applies one standard across public and private participants. It carries correction as far as the original alert traveled.

The central question is therefore simple:

Will the Payment Account framework regulate the actual risk at its genesis, or regulate the expanding consequences of an institutional reaction after the source event has disappeared from view?

ADDENDUM TO COMMENT

Docket No. OP-1878

Screening Triggers, Alert Validation, and Procedural Controls

The proposed framework should regulate the screening trigger at the beginning of the process. Accurate trigger design provides stronger protection than multiplying reactionary procedures after an unexplained alert enters the system.

The proposal authorizes additional assessments, attestations, audits, compliance meetings, account restrictions, and account closure based on perceived illicit-finance risk. Those procedures depend on the accuracy and classification of the original screening event. A false, stale, misclassified, or inadequately documented trigger can therefore produce an expanding series of compliance actions without improving payment-system security.

The Board should require Reserve Banks and Payment Account holders to distinguish among:

1. An exact sanctions-list match;

2. A potential or partial name match;

3. A geographic or jurisdictional alert;

4. A counterparty-based alert;

5. A transaction-pattern or behavioral alert;

6. A BSA/AML monitoring alert;

7. A terrorism-financing risk indicator;

8. An OFAC blocking requirement;

9. An OFAC rejection requirement; and

10. A general institutional-risk concern identified during account review.

These categories arise from different authorities, require different evidence, and lead to different responses. Combining them under the single label “illicit finance risk” obscures the origin and legal effect of the alert.

The Trigger’s Chain of Authority and Responsibility

Every material screening event travels through a chain of legal authority, institutional interpretation, technological implementation, and human judgment:

Statute or executive order → Treasury or OFAC program → specific list entry, legal restriction, or screening rule → bank or vendor screening engine → internal alert → assigned reviewer → clearance, rejection, blocking, restriction, or termination.

Each stage performs a different function. The statute or executive order supplies authority. Treasury or OFAC defines the applicable program. A list entry or screening rule identifies the prohibited or monitored condition. The screening engine compares source data against that condition. The reviewer interprets the resulting alert. The institution chooses the final disposition.

An auditable framework should preserve responsibility at every stage. The record should identify who supplied the data, who selected the rule, who configured the threshold, who interpreted the alert, who authorized the consequence, and who possesses authority to correct the result.

A trigger records that a system reacted. The complete chain explains why the system reacted and whether the reaction remained connected to the governing authority and verified facts.

Correction Must Travel as Far as the Alert

A correction process succeeds only when the correction reaches every system and participant that received the original classification. The framework should require institutions to:

Correct the originating source data;

Record the reason and effective date of the correction;

Identify every affiliated system, vendor, intermediary, Reserve Bank, or decision-making unit that received the alert;

Transmit the correction to each recipient;

Remove derivative alerts produced by the invalid classification;

Reconsider every restriction that relied upon the original alert; and

Restore access, status, and records affected by the invalid trigger.

An alert that travels farther than its correction remains an active source of institutional risk. Trigger governance therefore requires both controlled propagation and complete restoration.

Each material screening event should create an auditable record identifying:

* The date and time of the trigger;

* The system and screening vendor that generated it;

* The governing sanctions program, list, rule, or risk category;

* The version and effective date of the source data used;

* The data fields that produced the potential match;

* The trigger classification;

* The person or system that reviewed the alert;

* The information used to validate or clear it;

* Each escalation or routing decision;

* The final disposition; and

* The date and basis for removing any resulting restriction.

The Board should establish a uniform validation process before an institution imposes escalating consequences based on a screening alert. That process should confirm the source, classification, current status, materiality, and evidentiary basis of the trigger. Operational thresholds and detection methods may remain protected where disclosure would compromise system security, while the affected institution still receives the trigger category, governing authority, and factual basis necessary to respond.

The framework should also require periodic testing of screening systems for false positives, stale source data, mismatched identifiers, duplicate alerts, inconsistent classifications, and unnecessary propagation across affiliated systems. Institutions should preserve the original alert and every subsequent modification so reviewers can distinguish the initiating event from later conclusions derived from it.

A validated trigger supports focused action. An unvalidated trigger produces repeated document demands, duplicated reviews, expanding restrictions, and unnecessary compliance costs. Regulation at the trigger level would strengthen security, improve accuracy, preserve reliable audit trails, and reduce the need for layers of reactionary procedures.

The Board should incorporate trigger identification, classification, validation, correction, and closure standards into the Payment Account framework and the Account Access Guidelines.

SECOND ADDENDUM TO COMMENT

Docket No. OP-1878

Existing ACH Risk, Trigger Causation, and Equal Treatment

The payment system already accepts, prices, distributes, and controls the delayed-settlement risks associated with ACH transactions. Financial institutions regularly process ACH credits, debits, returns, reversals, and delayed adjustments through established risk-management systems.

The proposal characterizes those risks as incapable of mitigation for Payment Accounts without fully addressing the controls already used throughout the payment system. Those controls include prefunding, collateral, reserve requirements, transaction limits, exposure caps, delayed availability, return-risk reserves, monitoring, insurance, capital requirements, intraday liquidity, and supervisory intervention.

The Board should identify which controls it evaluated, the evidence supporting its conclusions, and why calibrated combinations of those controls would fail for Payment Account holders.

The proposed design creates a circular result. It removes access to intraday credit and other risk-management resources, then relies on the absence of those resources to justify excluding ACH access. The account design itself therefore creates part of the limitation later attributed to the applicant’s institutional risk.

A more complete analysis should distinguish between:

1. ACH credit originations that an institution can fully prefund;
2. ACH debit originations that create return exposure;
3. Consumer returns subject to extended time periods;
4. Reversals based on originating errors;
5. Unauthorized transactions;
6. Settlement failures caused by insufficient funds;
7. Operational or vendor failures; and
8. Fraudulent or intentionally improper activity.

Each category presents a different risk and supports a different control. A blanket exclusion prevents the Board from matching the control to the actual exposure.

Trigger causation

The proposal should also require institutions to determine what caused a screening or risk trigger before imposing escalating restrictions. A material

trigger may arise from intentional misconduct, inaccurate source data, a false-positive match, a stale sanctions entry, a vendor defect, a cybersecurity incident, an unauthorized third-party action, or an internal classification error.

Those causes carry different evidentiary meanings. A system-generated trigger should begin an examination of cause. It should not become its own proof of institutional risk.

For each material trigger, the institution should determine:

* Whether the triggering activity was intentional;

* Whether the account holder initiated or authorized it;

* Whether inaccurate or incomplete data produced the trigger;

* Whether a third party, vendor, intermediary, or compromised system caused it;

* Whether the trigger represents actual prohibited activity or a potential match;

* Whether the same trigger propagated through affiliated systems;

* Whether the institution corrected the originating data; and

* Whether any continuing restriction remains connected to a validated risk.

Micro-level consequences and institutional support

Traditional institutions operate within a structure that includes access to liquidity facilities, intraday credit, federal supervision, deposit-insurance mechanisms, established resolution procedures, and emergency governmental intervention. Those mechanisms absorb or distribute institutional risk at the system level.

A smaller Payment Account institution may receive no comparable support. Under the proposal, a single unvalidated trigger could instead produce repeated information demands, service restrictions, account closure, and loss of direct payment access. The institution and its customers would bear the consequences at the micro level even when faulty data, a vendor, an intermediary, or another institution created the trigger.

That asymmetry also creates system-level concentration risk. Excluding smaller institutions forces payment activity back through a limited number of large intermediaries. The resulting concentration increases dependency on institutions whose failure or operational interruption can affect the entire system.

Risk Reduction and Risk Transfer Require Separate Accounting

A control can reduce risk, retain risk, distribute risk, or transfer risk. Those outcomes carry different consequences and should receive separate treatment within the Board's analysis.

Risk is reduced when a control lowers the probability or expected magnitude of loss. Risk is retained when the institution knowingly accepts, measures, prices, monitors, and supports the exposure. Risk is distributed when several capable participants knowingly carry defined portions of the exposure. Risk is transferred when one participant removes the exposure from its own operational boundary and places it upon another institution, intermediary, customer, or community.

A transferred risk remains part of the payment system. Removal from one institutional ledger does not establish reduction of the underlying exposure. The Board should therefore measure the aggregate result across the complete payment chain rather than treating relief at one institutional boundary as proof of system-wide mitigation.

Payment Account restrictions may protect one Reserve Bank boundary while forcing smaller institutions to rely upon large intermediaries. That transfer can create additional fees, settlement delay, concentrated dependency, reduced transparency, interrupted access, and new operational failure points. The institution that appears safest at the first stage may have transferred the exposure to participants with less information, less bargaining power, and fewer corrective resources.

Institutional Boundaries Must Preserve Responsibility

Public comments concerning Regulation D have emphasized the importance of separating operational Payment Accounts from reserve-account relationships and preserving consistent Reserve Bank implementation. Clear boundaries serve an important purpose. They identify the legal character of the account and preserve the distinct functions of payment operations, reserve administration, and monetary policy. Those boundaries must also identify responsibility. When risk, data, or a classification crosses an institutional boundary, the receiving participant should know:

who created it;

what authority governs it;

what evidence supports it;

whether it has been independently validated;

who can correct it;

who bears the resulting exposure; and

how a correction will travel back through the chain.

Institutional-boundary preservation and continuous accountability reinforce each other. A boundary should clarify responsibility rather than provide the point at which responsibility disappears.

Additional questions

Add these to the existing questions:

Does the proposed control reduce aggregate payment-system risk or merely transfer it outside the Reserve Bank’s immediate boundary?

Which institution receives each transferred exposure, and what information and corrective authority accompany it?

Does forced dependence on large intermediaries create greater concentration and operational risk than controlled direct access?

When a transferred classification proves inaccurate, w

Questions requiring an answer

The Board should address:

1. What loss and return data establish that controlled ACH access presents an unacceptable risk for Payment Accounts?

2. Which combinations of prefunding, collateral, exposure limits, reserves, delayed availability, and transaction restrictions did the Board test?

3. Why can a Payment Account holder receive access to prefunded ACH credits only through an intermediary but not through equivalent direct controls?

4. What process will distinguish intentional activity from a false, defective, or third-party-generated trigger?

5. Who bears the loss when an inaccurate trigger restricts an institution’s payment access?

6. What correction, review, and restoration process protects an institution affected by a faulty trigger?

7. How does the Board compare the public support available to established institutions with the restrictions imposed on smaller eligible institutions?

8. Does excluding controlled ACH access increase concentration risk by preserving dependence on a small number of intermediaries?

Equal risk should receive equivalent treatment. Different account structures may justify different controls, but the framework should connect each restriction to measured risk, validated causation, and evidence that narrower controls cannot address the exposure.

The Board should regulate the actual risk, validate the initiating trigger, assign responsibility to the actor or system that created it, and provide a defined correction process before imposing expanding institutional consequences.

THIRD ADDENDUM TO COMMENT

Docket No. OP-1878

Screening-Level Auditability, Trigger Causation, and Institution-Created Risk

Meaningful risk management begins with an auditable screening event. The present framework gives institutions substantial authority to identify,

classify, report, escalate, and act upon a trigger while providing limited means to examine how the trigger arose or what interpretive lens transformed an event into a risk classification.

That structure creates space for arbitrary action, conflicts of interest, self-confirming conclusions, and restrictions imposed without meaningful notice or review.

The occurrence of an event establishes only that an event occurred. It does not establish:

* Why the system treated the event as a trigger;

* Which legal, regulatory, contractual, or model-based standard applied;

* Whether the underlying conduct was unlawful;

* Whether the conduct violated any account term;

* Whether the institution merely considered the conduct unusual;

* Whether inaccurate or incomplete data shaped the classification;

* Whether the reporting institution caused or provoked the event;

* Whether the event represented a lawful commercial remedy;

* Whether the screening model confused institutional inconvenience with illicit activity; or

* Whether the institution’s response created the risk later attributed to the affected party.

The applied lens requires examination

Every material trigger reflects an interpretive lens. That lens may arise from a sanctions list, an AML monitoring rule, a fraud model, a vendor algorithm, an institutional policy, a commercial-risk preference, adverse information, or a manual decision.

The audit record should identify that lens expressly. A general label such as “terrorism,” “illicit finance,” “high risk,” or “suspicious activity” cannot substitute for the underlying classification path.

A complete trigger record should answer:

1. What event occurred?

2. Who generated, initiated, or reported the event?

3. What source data entered the screening system?

4. Which system, model, list, policy, or rule evaluated the data?

5. What specific feature produced the alert?

6. Which classification did the system initially assign?

7. Did a person independently validate that classification?

8. What authority connected the event to the assigned risk category?

9. Did the underlying conduct violate any law or restriction?

10. Did the reporting institution possess a financial, procedural, or litigation interest in the classification?

11. Did the institution’s own action, delay, denial, routing decision, or data entry create or amplify the triggering condition?

12. Did the resulting restriction generate additional events that the system later treated as independent risk indicators?

Prior Notice Forms Part of the Trigger’s Genesis

A complete audit begins when the affected participant first gives notice of the underlying issue. It cannot begin only when the institution later generates an alert, records a missed payment, restricts an account, or assigns an adverse classification.

Prior notice may include:

a transaction dispute;

a request for inspection;

a demand for the governing instrument;

notice of inaccurate information;

a request for correction;

identification of unauthorized activity;

a complaint concerning goods or services;

an invocation of a contractual benefit;

a request for review; or

an effort to cure the underlying condition.

Each notice supplies context that can change the meaning of the later event. A missed payment following an unresolved dispute carries a different genesis from a payment abandoned without inquiry. An account irregularity following an uncorrected institutional error carries a different meaning from intentional misuse. A restriction imposed while a participant awaits a response may create the activity later characterized as additional risk.

The audit record should therefore identify:

Every material notice received before the trigger;

The date, recipient, and contents of the notice;

The office or person assigned to respond;

The institution’s investigation;

The records examined;

The response provided;

Any notice that remained unresolved when the adverse action occurred;

How the reviewer considered that prior notice;

Why the institution proceeded before resolving it; and

Whether the institution’s delay contributed to the triggering condition.

Notice Must Precede Institutional Finality

A smaller participant demonstrates engagement by giving notice and supplying information. The institution exercising adverse authority demonstrates accountability by addressing that notice before treating its own conclusion as final.

Every material adverse determination should state:

the operative rule;

the material facts;

the originating data;

the assigned reviewer;

the effective date;

the disposition of prior notices;

the available correction procedure; and

the conditions required for restoration.

An institution that omits the affected party’s prior notice from the decision record converts an incomplete chronology into an institutional conclusion. Genesis-level auditing restores the missing portion of the record.Institution-generated and institution-amplified risk

An institution that carries risk can also create risk. It can create or amplify risk through inaccurate data, defective screening rules, excessive matching thresholds, delayed corrections, conflicting system entries, unnecessary escalation, forced reliance on intermediaries, interrupted payment access, or restrictions that cause the very irregular activity the institution later identifies as suspicious.

This creates a self-confirming cycle:

1. The institution generates or interprets a trigger;

2. The institution restricts payment activity;

3. The restriction disrupts ordinary transactions;

4. The disruption produces unusual payment behavior;

5. The system labels the resulting behavior as additional risk; and

6. The institution cites the expanded alert history as confirmation of its original classification.

A valid audit must distinguish the original event from consequences created by the institution’s own response.

Lawful commercial activity

A commercial tool may exist specifically to protect an individual or smaller institution from improper conduct by a larger institution. Examples may include disputes, payment reversals, formal notices, regulatory complaints, security interests, demands for accounting, or other recognized commercial remedies.

Use of such a tool may be adverse to the institution’s financial or procedural interests while remaining lawful. A screening framework must distinguish:

* Unlawful conduct;
* Prohibited account activity;
* Legitimate fraud prevention;
* A commercial dispute;
* Exercise of a statutory or contractual right;
* Consumer or creditor protection activity; and
* Conduct that the institution merely finds inconvenient or unfavorable.

An institution should not control the commercial relationship, activate the trigger, define the meaning of the trigger, and then use that internally generated classification as conclusive evidence against the affected party.

Independent audit and review

The Board should require independent review when a trigger produces material consequences, including delayed settlement, service restrictions, enhanced reporting, account closure, or denial of Reserve Bank access.

That review should have access to:

* The original source data;

* The screening system and rule version;

* The trigger category;

* The model or matching logic;

* The complete audit history;

* Changes made after the initial alert;

* Communications among the reporting, screening, and decision-making actors;

* Any financial or procedural interest held by the reporting institution;

* The factual basis for escalation;

* The institution’s contribution to the triggering event; and

* The final correction or clearance record.

Operational details that would permit evasion of legitimate screening may remain protected. An affected institution should still receive meaningful notice identifying the event, general trigger category, governing authority, material facts, resulting restriction, correction procedure, and responsible decision-making unit.

Procedural safeguards

A screening classification that affects payment access requires:

1. A preserved audit trail;

2. Separation between reporting and final decision-making;

3. Review of the reporting institution’s role in creating the event;

4. A determination of whether the underlying conduct was unlawful;

5. A defined process for submitting corrective information;

6. Independent review of disputed classifications;

7. A deadline for validation or clearance;

8. Removal of derivative alerts produced by an invalid original trigger; and

9. Restoration of access when the institution cannot validate the classification.

Risk analysis must examine both sides of the transaction. It must evaluate the applicant’s conduct and the screening institution’s conduct. It must measure external risk and risk created within the screening process itself.

A framework that audits only the subject of the trigger leaves the trigger-producing institution outside the risk analysis. Effective oversight requires examination of who created the trigger, what lens gave it meaning, whether the conduct was unlawful, whether the reporting actor had a conflicting interest, and whether the institution created the risk it later claimed to mitigate.

FOURTH ADDENDUM TO COMMENT

Docket No. OP-1878

Consumer-Protection Activity and Asymmetric Attribution of Risk

Consumer-protection mechanisms exist to protect individuals from institutional misconduct, error, overreach, and unequal control over information and payment systems. The use of a lawful consumer-protection mechanism should prompt examination of the underlying dispute and the institution’s conduct that preceded it.

The current risk framework can reverse that purpose. An individual invokes a dispute right, payment remedy, correction procedure, regulatory complaint, accounting demand, or other commercial protection. The institution then labels that action as unusual, adverse, suspicious, or risky. The individual’s protective action becomes the trigger, while the institutional conduct that caused the individual to act disappears from the analysis.

The resulting attribution resembles a mouse moving through a room filled with elephants. The elephants react, destroy the room, and attribute the destruction to the mouse because its movement came immediately before their reaction. That sequence identifies timing. It does not establish causation or proportional responsibility.

A complete risk analysis must examine:

1. The institution’s conduct before the consumer acted;

2. The reason the consumer invoked the protective mechanism;

3. Whether the consumer used a lawful commercial or regulatory process;

4. Whether the institution classified protected activity as a risk indicator;

5. Whether the institution’s response was proportionate to the original event;

6. Whether the institution’s response created additional financial or operational disruption;

7. Whether that disruption generated further alerts;

8. Whether the institution treated those derivative alerts as independent confirmation;

9. Whether the institution benefited from assigning responsibility to the consumer; and

10. Which actor possessed the authority and practical ability to prevent the resulting harm.

Reciprocal Notice in Commercial Relationships

Financial institutions require members and borrowers to provide timely notice, accurate information, complete documentation, and prompt responses. Those requirements establish the institution’s own standard for responsible commercial conduct. The same standard should govern the institution when a member disputes an obligation, requests inspection of an instrument, seeks correction of inaccurate information, or asks for the reason supporting an adverse determination.

My documented experience with a regulated credit union illustrates the contradiction. I submitted written inquiries concerning a vehicle transaction and requested inspection of the instrument upon which the credit union claimed its collateral interest. I retain the emails establishing those requests and the institution’s responses. While those notices remained unresolved, the credit union exercised the greater institutional power: it treated the account adversely and expelled me from membership before providing notice sufficient to identify the governing violation, the complete factual basis, the assigned reviewer, and a meaningful opportunity to present the transaction record before the action took effect.

The institutional record captured the adverse payment condition and the expulsion. A complete record must also capture:

the vehicle-related inquiries preceding the payment dispute;

the request to inspect the claimed instrument;

the credit union’s response;

the unresolved status of those notices;

the institution’s reason for proceeding before answering them;

the evidence considered by the decision-maker;

the correction process offered before expulsion; and

every system or recipient that later received the resulting classification.

This experience presents the regulatory issue without asking the Board to adjudicate the underlying commercial dispute. It demonstrates how a financial institution can demand notice and performance from the member while treating its own duty to answer, disclose, investigate, and correct as secondary.

The Commercial Contradiction

An institution cannot credibly demand:

Timely notice while leaving the member’s notice unanswered;

Documentary support while withholding the instrument supporting its own claim;

Honest disclosure while withholding the operative reason for an adverse action;

Corrective conduct while providing no identified path to cure;

Contractual performance while preventing meaningful review of the governing instrument; and

Accountability from the member while insulating its own decision from equivalent examination.

Commercial notice must carry reciprocal effect. When the affected party provides notice, the institution should acknowledge it, preserve it, investigate the facts identified in it, incorporate it into the decision record, and address it before converting the disputed event into a final adverse classification.

The Elephant’s Response and the Bee’s Movement

The earlier mouse-and-elephant comparison can be developed more accurately through the relationship between bees and elephants. A small source event may cause a powerful institutional actor to move quickly in self-protection. The institution controls the scale and direction of its response. Its reaction may affect accounts, payment access, commercial relationships, and downstream classifications far beyond the original event.

The bee explains the immediate stimulus. The elephant's size, force, route, and institutional control explain the resulting damage. A complete audit examines both.

Risk analysis should therefore determine:

what caused the initial movement;

whether the perceived threat was accurately identified;

whether the response remained proportional;

whether the institution had safer alternatives;

whether the reaction displaced risk onto others; and

who possessed the practical power to prevent or correct the resulting harm.

The actor with greater control carries the greater duty to account for the design, accuracy, scale, and consequences of its response.

Institutional contribution must form part of the audit

A screening institution should document its own contribution to the event. The audit should begin before the trigger and preserve the full chronology rather than beginning when the affected person exercised a protective right.

The analysis should ask:

* Which institutional decision created the underlying dispute?

* What information did the institution possess before the trigger?

* Did inaccurate, incomplete, or conflicting institutional records contribute?

* Did the institution deny or delay an available correction process?

* Did the institution's restrictions create the later irregular activity?

* Did the institution select an interpretive lens that favored its own financial or procedural position?

* Did the institution investigate its own systems and personnel with the same intensity applied to the affected person?

Proportionality and responsibility

The actor with greater system control also possesses greater capacity to create, prevent, amplify, or correct harm. A meaningful risk framework must therefore examine responsibility in proportion to institutional control.

A consumer's action may provide the occasion for an institutional response. The institution remains responsible for the design, scale, accuracy, and consequences of that response. Automated systems, compliance obligations, and internal policies do not erase institutional choice. They document how the institution exercised that choice.

Consumer-protection activity should receive a distinct classification within the screening framework. Before escalating such activity, the institution should establish:

1. The underlying action was unlawful or actually prohibited;

2. The trigger did not arise merely because the consumer challenged the institution;

3. The institution investigated its own role in creating the event;

4. The response remained proportional to the validated risk;

5. An independent reviewer examined any institutional conflict of interest; and

6. The process provides correction, restoration, and responsibility for institution-created harm.

A system that examines only the mouse will always conclude that the mouse caused the room to collapse. A reliable system examines the elephants, the architecture of the room, the force of the response, and who possessed control over the resulting destruction.

This can relate even to the Governments own practices during the peaceful transition of one administration entering and one leaving there is a 90-day window of almost zero accountability. Specifically, 98 billion dollars left the government accounts during that 90-day window. Does the leaving administration accountable That? Are those figures accounted for in risk factors, are sections handed out?

In closing;

Behavioral Change Requires the Rod

If the Board intends to change behavior, it must avoid controls that place the staff in the hand where the rod belongs.

Punishment operates through the anticipation of pain, deprivation, exclusion, or loss. It creates fear and anxiety before the institution ever applies the threatened consequence. That anticipation may compel submission, but submission produced by fear does not establish understanding, correction, or safer behavior.

The rod serves a different purpose. It corrects direction. It identifies the departure, redirects the recipient, and changes the trajectory before greater harm occurs. Its success appears through restored alignment rather than inflicted pain.

An institution cannot convert punishment into correction merely by administering it through a compliance system.

Account restrictions, unexplained delays, repeated information demands, financial isolation, propagated risk classifications, and threats of closure may operate as the staff even when the institution labels them "risk controls." Their actual character depends upon their design, force, duration, purpose, and effect.

A behavior-changing framework should provide:

1. Meaningful notice of the conduct requiring correction;

2. Identification of the governing standard;

3. A clear explanation of the desired behavior;

4. An opportunity to correct inaccurate information;

5. A proportionate and graduated response;

6. Separation of guidance from defensive force;

7. Independent review before severe restrictions;

8. A defined duration for every corrective measure;

9. Restoration after the condition has been corrected; and

10. Audit of fear, disruption, and collateral harm created by the control itself.

The staff belongs where the institution has validated a genuine external threat requiring defensive force. The rod belongs where conduct requires clarification, correction, redirection, or restored compliance.

An ambiguous trigger cannot decide which tool the institution uses. That decision requires human judgment, source-level audit, causation analysis, proportionality, and review of the institution's own contribution.

The Board should give these distinctions serious and respectful consideration if it intends to enter the business of changing behavior. A framework that seeks changed behavior must measure whether its controls produce understanding and correction or merely fear and submission.

Correction changes the recipient’s trajectory.

Punishment changes the recipient’s expectation of pain.

A responsible institution must know which result it intends, which tool it has placed in its hand, and whether that tool still serves the protective purpose for which the institution received its authority.

The Human Element: The Rod and the Staff

The elephant at the threshold of escape acts through self-preservation. It does not stop to measure collateral damage. It moves with the herd, and everything within the path of that movement bears the consequences.

People, however, are hardly ever described through the character of elephants. History, faith, and common experience more often compare human behavior to sheep.

Sheep wander. They follow the animal immediately in front of them. One misdirected movement can redirect the flock. Left without guidance, their individual movements combine into disorder. The danger does not arise because every sheep intends harm. It arises because movement spreads through imitation, proximity, and the absence of direction.

That is where the human element enters the risk analysis.

A human institution can observe the flock, understand why it moved, identify who moved first, determine what influenced that movement, and distinguish confusion from danger. It can guide, correct, protect, and restore order. Its authority carries responsibility because it can understand consequences that an escaping elephant cannot.

The shepherd carries both a rod and a staff because correction and protection require different tools.

The rod is short and thin. It is designed for guidance and correction rather than force. The shepherd uses it to redirect movement, establish boundaries, and bring the wandering member back into alignment with the flock. Its purpose is behavioral correction and restored order.

The staff is long and thick. It creates distance between the flock and an approaching external threat. Its length permits the shepherd to confront wolves, bears, and other dangers while remaining positioned between the threat and those under protection. It can be swung with speed, weight, and force because it serves a defensive purpose.

The rod guides the flock.

The staff confronts the threat.

correction and punishment are different institutional acts. Correction seeks understanding, changed behavior, and restoration. Punishment anticipates pain, deprivation, exclusion, or fear as the means of compelling submission.

A shepherd honors the entrusted position by selecting the tool according to the actual hazard. A wandering sheep receives the rod's guidance. An attacking wolf receives the staff's force.

When the institution uses the staff against the sheep, guidance becomes punishment. A tool intended to protect the flock from external danger becomes an instrument of force against the population it was designed to protect.

When the institution uses the rod against a genuine external threat, the institution fails to protect the flock.

Auditability determines which tool the event requires.

The audit must begin at the hazard's genesis. It must identify what occurred, why it occurred, whether the conduct was lawful, whether the actor intended harm, whether institutional conduct contributed to the event, and whether the condition requires correction or defensive force.

Without that source-level audit, the institution can label a wandering movement as an attack and apply the staff where the rod was required. The institution can then describe the resulting pain, disorder, and resistance as further evidence that the flock presented a danger.

That creates another self-confirming cycle:

1. A member of the flock moves;

2. The institution classifies the movement as a threat;

3. The institution applies defensive force;

4. The force creates pain and disorder;

5. The disorder spreads through the flock; and

6. The institution cites the spreading disorder as proof that its original use of force was necessary.

The resulting chaos does not validate the original classification. It may instead document misuse of the control.

A legitimate risk framework must preserve the separation between guidance and force, correction and punishment, internal disorder and external threat. It must identify who selected the tool, what facts supported that selection,

whether the response remained proportional, and whether the institution used authority for its appointed purpose.

The shepherd dishonors the position when the tools become interchangeable. The risk of abuse rises whenever a protective institution can use the staff against the flock, call the resulting disorder a threat, and leave its own use of force outside the audit.

Genesis: The Trigger Is Not the Explanation

Statute or executive order → Treasury or OFAC sanctions program → specific list entry or screening rule → bank or vendor screening engine → internal alert → assigned reviewer → clearance, rejection, blocking, restriction, or account termination.

That chain identifies how an alert travels. It still leaves the controlling question unanswered: What caused the conduct that the institution later classified as a violation?

My reported expulsion from Citizens Bank represents the genesis of that question. The institution revoked access before giving me notice and a meaningful opportunity to present the facts. An agency framework built upon notice, documentation, and review should examine whether the institutions operating beneath that framework extend those same protections to the individuals and smaller institutions affected by their decisions.

The stated reason for an adverse action may appear sufficient during a surface-level regulatory review. A valid audit must go further. It must examine the event that produced the trigger, the lens applied to that event, the information available to the institution, and the conduct of every participant whose actions contributed to the result.

Consider the automobile account. Why would a borrower earning approximately $80,000 to $100,000 annually suddenly stop making payments? That question requires investigation before the missed payment becomes the entire story:

Did the borrower make good-faith inquiries concerning the vehicle?

What defects did the borrower report?

How did the dealer respond?

Were the inquiries supported by the vehicle’s condition?

Did the dealer restrict the scope of inspection?

Would an independent inspection have revealed the reported defect?

What was the cost of repair compared with the vehicle’s sale price and value?

Did the lender examine the underlying dispute before treating nonpayment as proof of unwillingness or heightened risk?

Did the resulting classification travel into other systems and influence later adverse decisions?

A missed payment is an event. It does not establish its own cause. The distinction between a borrower who refuses an honest obligation and a borrower who disputes a materially defective transaction matters when the stated purpose of the framework is behavioral correction.

Banks expect borrowers to act honestly, disclose material information, honor agreements, and cure defaults. Dealers, lenders, banks, vendors, and regulators should operate under the same moral standard. A system cannot demand morality in borrowing while ignoring morality in selling, servicing, lending, screening, and enforcement.

The proper inquiry therefore extends beyond: Was a rule triggered? It must ask:

Why was the rule triggered, who contributed to the triggering event, what facts were considered, what facts were excluded, and did the affected person receive a meaningful opportunity to correct the record before punishment spread through the system?

Behavior cannot be responsibly changed when the system audits only the person who received the punishment. Accountability begins at the genesis of the event and follows every participant through the final disposition.

fact strengthens the genesis inquiry because it shows sought verification before the dispute became a payment/default classification.

Use precise language identifying the instrument the bank claimed created or evidenced its security interest—such as the retail installment contract, security agreement, title record, or lien document.

Refusal to Permit Inspection of the Claimed Instrument

Before the account was characterized through nonpayment, default, or risk terminology, I made documented good-faith requests to inspect the instrument upon which the bank claimed its collateral interest in the vehicle. The bank refused or failed to provide a meaningful opportunity for that inspection. I retain the emails documenting my requests and the institution’s responses.

That sequence matters. It raises factual questions that should precede any judgment about my conduct:

What instrument did the bank rely upon?

Did the bank possess the original, a copy, or an electronic record?

What language allegedly created the security interest?

What vehicle and obligation did the instrument identify?

Who executed, transferred, or maintained it?

Why was inspection refused?

Did the bank record my requests in the servicing or claim file?

Did anyone investigate the requested verification before classifying the account?

Was the resulting default or risk classification transmitted to another institution, vendor, reporting system, or regulator?

The record therefore presents more than a missed payment. It presents a documented request to verify the instrument, the institution’s response to that request, and the later treatment of the account. A complete review must examine that sequence before assigning motive, fault, or risk.

When Punishment Replaces the Lesson

My father has occupied the same chair in the same church for fifty years. His convictions have remained equally fixed. When I was young, punishment followed whether I admitted the truth or denied it. In his view, God’s law required correction, and the consequence would arrive when he returned home.

The intended lesson concerned truth, responsibility, and ownership of one’s actions. Yet the certainty of punishment changed the lesson. The question in the child’s mind became: How do I avoid punishment? Fear displaced reflection. Concealment became safer than honesty. Avoiding detection became more important than correcting conduct.

Institutions can produce the same result. When every trigger leads toward restriction, exclusion, or anticipated pain, the regulated party learns to manage the trigger rather than understand the rule. It learns what to hide, how to remain below a threshold, and how to avoid attracting institutional attention. That is compliance through fear. It creates outward submission without cultivating responsibility.

A framework designed to change behavior must preserve a meaningful distinction between confession and concealment, error and misconduct, correction and punishment. Honesty must open a path toward cure. Cooperation must carry value. Proportionality must remain visible. Otherwise, the institution teaches avoidance while claiming to teach accountability.

The measure of a successful control is not whether it makes people fear being caught. The measure is whether it helps them understand the standard, accept responsibility, correct their trajectory, and return to lawful participation.

The Rod or Staff

People have historically been compared more closely to sheep than to elephants. Sheep wander, follow the one immediately before them, and create disorder when guidance disappears. The shepherd therefore carries both a rod and a staff, each designed for a different purpose.

The rod is short and thin. It guides, corrects, and changes the trajectory of a member of the flock. Its purpose is redirection. The staff is long and thick, designed to create distance and deliver forceful blows against wolves, bears, and other validated threats to the safety of the flock.

The distinction between those instruments must remain clear. If the Board intends to cultivate responsible behavior, it must avoid controls that place the staff in the position reserved for the rod. An unexplained trigger, unresolved notice, disputed transaction, incomplete record, or correctable deficiency calls for examination and guidance. A validated external threat may justify forceful containment. The trigger must be understood before the institution selects the tool.

When the staff occupies the rod's place, correction becomes punishment. Financial pain, exclusion, account restriction, payment interruption, and propagated risk classifications create fear and anxiety through the anticipation of institutional force. That fear may produce immediate obedience, but obedience motivated by pain differs from understanding, responsibility, and correction.

When the rod occupies the staff's place, the framework also fails because a validated external threat receives an inadequate response. Effective governance requires the right instrument, applied to the right condition, by an accountable decision-maker, for a defined purpose and duration.

The Board should therefore require each material control to identify:

the conduct requiring correction;

the validated threat, if one exists;

the reason the selected response fits that condition;

the corrective behavior expected from the participant;

the opportunity and time allowed for correction;

the point at which guidance may become containment;

the reviewer authorizing that transition; and

the conditions required for restoration.

The rod changes trajectory. The staff protects against a validated threat. A responsible framework keeps each instrument in its proper place.

Punishment imposed physical pain. Discipline would have required confrontation of the consequence of the conduct, repair what was damaged, and understand why the rule existed. The distinction matters because each method teaches a different lesson.

Consider a child caught drawing on a wall. The parent becomes angry, and the child feels fear. The parent sends the child to a room until the child learns how to behave. While the child sits there anticipating punishment, the parent fills a bowl with hot water, takes a sponge, and removes the marker from the wall.

The child experiences fear and isolation. The parent experiences the actual consequence of the child's conduct. The parent cleans the wall. The child returns to their room having learned that getting caught produces punishment while someone else repairs the damage.

Discipline places the sponge in the child's hand.

Cleaning the wall connects conduct to consequence. The child sees the damage, performs the labor required to repair it, and understands why the rule exists. Responsibility becomes part of the lesson. Correction changes the child's trajectory because the person who created the condition participates in restoring it.

Financial regulation faces the same choice.

Account restrictions, payment delays, exclusion, adverse classifications, and financial loss can impose pain. They can create immediate compliance through fear of institutional consequences. Behavioral correction requires something more: accurate notice, identification of the governing standard, an opportunity to understand the violation, a meaningful path to cure, responsibility for the resulting harm, and restoration after correction.

closing;

Comparative Regulatory Design: Accountability Follows Influence

Contemporary financial-regulation proposals outside the United States provide a useful comparison. The United Kingdom Financial Conduct Authority's 2026 Consumer Duty consultation focuses responsibility upon each firm's role, activities, and ability to influence customer outcomes throughout a distribution chain. It rejects a structure in which the participant nearest the customer carries responsibility for the entire chain while upstream firms, information providers, and outsourced service providers remain outside the analysis.

That approach recognizes several principles relevant to Payment Account governance:

Responsibility should follow the actor's role and practical influence over the outcome;

Information must travel across the distribution chain;

A firm should identify risks created by its own activities;

Complaints require root-cause analysis rather than treatment of symptoms alone;

Records should identify the problem, selected intervention, responsible actor, and resulting outcome;

Outsourcing does not sever institutional accountability; and

Remedial action should address the condition that produced harm.

These principles reinforce genesis-level auditing. A Reserve Bank, account holder, intermediary, screening vendor, and reporting institution should each account for the activity it controlled and the consequences it produced. The final reviewer should receive the complete decision chain rather than a conclusion detached from its source.

A framework that assigns responsibility according to institutional influence can distinguish applicant-created risk from risk created by screening rules, vendor data, delayed responses, or institutional restrictions. It can also identify which participant possesses the information and authority necessary to correct the originating condition.

Meaningful Notice Requires Actionable Information

Regulatory simplification should distinguish disclosure volume from meaningful notice. Long, technical disclosures can obscure the information a participant needs to understand and respond to an institutional decision. Effective notice identifies the operative event, governing standard, material facts, responsible decision-making unit, consequence, response deadline, corrective procedure, and conditions for restoration.

A smaller participant should not receive pages of general policy language while the institution withholds the specific reason for adverse action. The relevant measure is whether the information enables timely understanding, informed response, correction, and review.