FORMAL NOTICE OF SYSTEMIC FALSE-POSITIVE ACCOUNT SUSPENSIONS AND REQUEST FOR REMEDIAL ACTION

November 15, 2025

Meta Platforms, Inc.
1 Hacker Way
Menlo Park, CA 94025
USA

From: Shohei KIMURA (holder of a Meta Verified badge)
Facebook Account URL: (https://www.facebook.com/profile.php?id=61572398409812)

I submit this legal notice regarding repeated erroneous enforcement actions taken against my Facebook account and the recurring destructive data processing that has followed those actions. This notice requests formal clarification and corrective measures. Issued under applicable international copyright obligations and general principles of tort liability, this Letter constitutes a formal notice of rights, systemic injury, and remedial demand.

Ⅰ. Background of Prior Incidents
On July 23, 2025 (JST), my account was wrongly subjected to permanent suspension. It was silently restored in early September without any explanation, despite my written request for one.
Subsequently, on November 10 and November 12, 2025 (U.S. time), my account was again subjected to erroneous automated enforcement, triggering a mandatory selfie-video identity check. While the identity review was completed immediately, the same destructive post-restoration processing occurred again.

Ⅱ. Harmful Post-Restoration Processing
After each erroneous enforcement action—and separate from the enforcement itself—my account has been subjected to the following irreversible data resets:

● A full zero-reset of all reactions except "likes" on pages, "likes" on followed pages, and comments
● Complete removal of all previously followed accounts and pages
● Temporary blocks that prevent me from restoring my follow list, despite my actions being manual, legitimate, and verified

These are not security-essential processes. They constitute avoidable destruction of digital property.

III. Legal Characterization

The repeated deletion of account-level relationship data, after an erroneous enforcement event, constitutes:

● Destruction of long-maintained relational data
● Foreseeable and preventable harm unrelated to fraud prevention
● A persistent systems-level malfunction that Meta has failed to correct

These actions collectively amount to injurious conduct resulting in material impairment of digital assets.

IV. Disclosure of User Characteristics Leading to False Positives

I am a Meta Verified user with highly structured posting activity, multilingual output, extensive ad review behavior, and frequent organization of follows and page relationships. These patterns are entirely legitimate and manually executed.

Because such behavior is predictably misclassified by automated detection models, Meta should have taken reasonable steps to prevent recurrent harm, including preventing post-restoration destructive processing.

Ⅴ. Required Clarifications

Meta is required to provide a formal written response addressing:

● Why destructive zero-reset processing is executed after erroneous enforcement
● Whether Meta intends to continue executing such processing in the future
● What corrective actions will be implemented to prevent further damage

VI. Response Deadline

A formal written response must be postmarked no later than January 15, 2026. If no response is received by that date, the matter shall be deemed "unanswered" as of February 15, 2026. Upon classification as "unanswered," Shohei KIMURA will treat this systemic matter as an active disputed case, suspend all further dialogue, and decline any future negotiations concerning licensing fees or rights related to the intellectual property embedded in the Formalization Procedure of Thought and in the theoretical framework provisionally designated as "Human Civilization Software Update 3.0".

VII. Reservation of Rights

I reserve all legal rights and remedies pertaining to the damages already incurred and any further damages resulting from Meta's automated systems.

Sincerely,
Shohei KIMURA (holder of a Meta Verified badge)
Representative, bitBuyer Project (ak4dy1@gmail.com)

APPENDIX
Technical Proposal for an iPhone Biometric "Trusted Device" System to Prevent False-Positive Account Suspensions

Although this document is attached as an APPENDIX, it contains the substantive terms that will ultimately determine whether this matter resolves cleanly or proceeds toward unnecessary escalation.

Purpose
This appendix outlines a technical and operational solution designed to prevent false-positive automated suspensions triggered when high-volume user actions resemble bot-like behavior. The proposal leverages iPhone-based biometric authentication (Face ID / Touch ID) to establish a persistent, verifiable "trusted device" link between a verified user and Meta services. This system significantly reduces computational load, minimizes the need for human review, and ensures uninterrupted service availability for verified users.

Ⅰ. Background and Problem Statement
Across Meta platforms, certain high-frequency user actions—such as rapid advertisement feedback, batch feed optimization, or accelerated follow management—can be programmatically misinterpreted as automated or malicious behavior. When this occurs, the system may:

● Trigger an automated account suspension
● Require submission of a selfie-video for identity verification
● Impose processing delays of up to one hour or more
● Restore access only after all recent account actions are rolled back

For verified users, this workflow represents a disproportionate interruption, creates substantial data inconsistency, and places unnecessary load on Meta's internal review systems.

Ⅱ. Overview of the Proposed Solution: iPhone Trusted Device Enrollment
This proposal introduces a Trusted Device Enrollment Mechanism for verified accounts, relying on iPhone biometric authentication as a secure, low-overhead identity anchor.

Core Components
1) Biometric Identity Binding: Upon enrollment, the Meta app requires a Face ID or Touch ID authentication. The resulting authentication token is paired with the verified Meta account via secure cryptographic handshake.
2) Long-Term Trust Anchor: The trusted status persists on the device until explicitly revoked by the user or Meta.

3) Real-Time Biometric Challenges: When high-volume actions exceed defined behavioral thresholds, the app triggers an immediate biometric verification request instead of issuing an automated suspension.

III. High-Volume Action Threshold Handling
Instead of suspending the account, Meta may invoke lightweight biometric challenges based on server-side detection of high-frequency behavior. Examples include:

● Processing 50+ ad feedback actions within 60 seconds
● Rapid removal or organization of follow targets
● High-speed scrolling behavior coupled with action triggers
● Any pattern statistically similar to bot automation

When thresholds are crossed, the user receives:
    "Identity verification required to continue. Please complete Face ID authentication."
This mechanism provides immediate, cryptographically strong confirmation of real-time user presence and eliminates the need for selfie-video review queues.

IV. Extension to Desktop (macOS / Windows)
When Meta systems detect bot-like actions originating from a desktop environment, a cross-device challenge is issued:
        "To continue, please complete biometric verification on your iPhone."
The security model mirrors multi-factor systems already deployed by Apple, Google, and major financial institutions.
Even if macOS supports Touch ID, iPhone Face ID remains the universal high-assurance verification method for continuity and standardization.

Ⅴ. Android Device Handling
Given ecosystem fragmentation—root access, OEM variance, and susceptibility to automation—Android devices cannot be treated with the same trust level as iOS.
Therefore:

● iPhone → High-Assurance Trusted Device Mode
● Android → Standard Mode (biometric challenges occur more frequently)

This tiered model maintains fairness while properly accounting for differences in platform reliability and attack surfaces.

VI. Security, Operational, and Resource Benefits
1. Reduction of False-Positive Suspensions: Real-time biometric confirmation removes ambiguity around high-volume actions.

2. Elimination of Selfie-Video Review Bottlenecks: Human review workload and server processing overhead are drastically reduced.
3. Superior User Experience: The verified user never loses account visibility, and service continuity is preserved.
4. Strengthened Platform Security: Bot networks and fraudulent clusters cannot pass biometric challenges and are naturally filtered out.
5. Reinforcement of Verification Badge Value: Verified users receive security proportional to their identity-verified status.

VII. Implementation Feasibility
All required capabilities already exist within:

● Apple Secure Enclave
● App-level Face ID / Touch ID invocation
● Cross-device multi-factor prompts
● Standard OAuth-based bindings

No novel hardware, platform changes, or burdensome server-side structures are required.

VIII. Conclusion
The proposed system meets Meta's priorities of:

● Reducing operational cost
● Increasing account security
● Preventing user-facing service failures
● Blocking malicious automated actors
● Maintaining consistent platform integrity

And it achieves all of the above without adding computational strain or requiring additional human reviewers.
For verified users—whose accounts represent elevated trust and public identity—the introduction of a Trusted Device Biometric System would significantly strengthen Meta's reliability and credibility.

IX. Comparative Assessment of Existing Identity Verification Methods, User-Experience Impact, and Technical Advantages of the Proposed Face ID–Integrated Architecture

For purposes of this APPENDIX, Meta is hereby informed that the identity-verification framework outlined below constitutes a technically novel, industrially applicable, and patent-realizable architecture. The comparison is presented to establish the substantial UX, operational, and cost-efficiency advantages of the proposed method over Meta's current selfie-video–based verification workflow.

1) Background: Limitations of Meta's Existing Selfie-Video Verification Process
● Meta's present verification mechanism relies on server-side ingestion, parsing, classification, and adjudication of user-submitted selfie videos.
● This workflow routinely results in verification delays extending up to one hour, particularly when false negatives require manual review or secondary checks.
● Each such delay disrupts account continuity and imposes an operational burden that is non-scalable under global user loads.
● The architecture further entails a persistent cost problem: video-based identity assessment requires ongoing server computation, storage capacity, load-balancing overhead, and, in many cases, human review.
● The mechanism is structurally incompatible with user expectations in contemporary social networking culture, where individuals—especially those who maintain personal branding—prefer to appear younger, more polished, or stylistically consistent. The requirement to record real-time, unfiltered video introduces significant psychological resistance and UX degradation.
● Consequently, Meta incurs both reputational UX friction and escalating operational cost with no corresponding improvement in verification reliability.

2) UX Impact and Functional Drawbacks
● A single false-negative determination under the current system typically yields a multi-step re-verification cycle, producing service interruptions measurable in tens of minutes to over an hour.
● Verification interruptions propagate outward into Meta's ecosystem, affecting Content Integrity systems, Commerce surfaces, advertiser trust signals, and the visibility ranking of high-engagement accounts.
● These interruptions are especially damaging for accounts with authentication badges, whose economic and reputational activities depend on continuous operational availability.
● The workflow additionally risks short-term data coherence instability, as identity challenges may occur mid-session, requiring rollbacks or internal state reconciliation that further degrade UX.

3) Proposed Solution: Instantaneous Face ID–Integrated Local Authentication
The architecture described in this APPENDIX introduces a fundamentally distinct verification paradigm:

● All identity matching and liveness confirmation occur locally on the user's device via Face ID–class biometric hardware security modules.
● The device reports only a binary verification result to Meta's servers; no biometric template, image, or video is transmitted.
● End-to-end authentication occurs in under a second, comparable to passing through a transportation ticket gate, and does not interrupt ongoing app interactions.
● Localized computation eliminates the need for server-side video ingestion, storage, and inferential evaluation.

● Meta's operational cost per verification approaches zero, as server responsibilities are reduced to receipt-of-result and state update only.
● The authentication step is unobtrusive and can occur contextually, such as when opening Creator tools, accessing Ads interfaces, or performing commerce-authenticated actions, without perceptible UX degradation.
● Because no selfie video is required, users experience no psychological friction, no performance anxiety, and no concern about appearing older, tired, or visually inconsistent with their preferred self-presentation.

4) Comparative Technical Advantages
The proposed method yields measurable superiority across all relevant engineering dimensions:

● Latency: reduced from minutes or hours to sub-second.
● Server Load: reduced from continuous GPU/CPU inference to negligible.
● Scalability: improved from throughput-constrained to near-infinite device-distributed processing.
● Privacy: improved through zero video transmission and localized biometric matching.
● Reliability: significantly higher due to hardware-rooted security modules and near-zero false negatives under stable sensor conditions.
● UX Continuity: maintained at all times; no workflow interruption occurs during verification.
● Economic Efficiency: total cost of ownership for Meta decreases dramatically, as the solution externalizes the compute burden to user devices.

5) Patent Realizability and Novelty Considerations
● This framework constitutes more than a mere substitution of biometric modality; it introduces a system architecture in which server-side identity assurance is achieved without server-side biometric handling.
● The combination of (i) instantaneous local hardware-secured facial authentication, (ii) ephemeral binary-result transmission, and (iii) in-session seamless UX integration represents a non-obvious improvement over established verification art.
● Under prevailing standards in multiple jurisdictions, including Japan and the United States, the described system possesses clear technical character and industrial applicability.
● As such, Meta is hereby notified that the contents of this section may support patent claims or related intellectual-property assertions by the author, depending on the trajectory of any future dispute or negotiation concerning this APPENDIX.

6) Consequences for Meta's Platform Strategy
● Adoption of this architecture would eliminate the majority of operational costs associated with selfie-video verification.
● It would materially improve trust, badge prestige, and creator retention due to the seamless nature of authentication.

● Conversely, failure to adopt such architecture carries long-term competitive risk, as platforms implementing this method would enjoy superior UX, trustworthiness, and operational efficiency.

● For these reasons, Meta is expected to treat the contents of this section as technically substantive and commercially material to its identity-verification roadmap.

This IX constitutes the formal technical and comparative foundation upon which the licensing terms described elsewhere in this APPENDIX are predicated.

Ⅹ. Copyright Status, Jurisdiction, Authorial Authority, and Formalization Rights

Prior to addressing the licensing terms, Meta is hereby placed on explicit notice that all subsequent sections constitute legally operative and enforceable assertions of authorship, ownership, and procedural rights.

1. Pursuant to Japanese copyright law and all Berne Convention signatory jurisdictions, the conceptual propositions, descriptive formulations, structural diagnoses, procedural articulations, and technical prescriptive statements contained in this APPENDIX have already acquired full copyright protection as the authored work of Shohei KIMURA. While Meta remains free to develop, study, or technically implement the underlying ideas described herein, all expressive forms—including the structural articulation, procedural exposition, conceptual framing, and descriptive methodology—are protected without exception. Any reproduction, quotation, derivative expression, internal documentation, policy integration, or technical drafting, regardless of medium or jurisdiction, requires the author's explicit prior written authorization.

2. Meta is hereby placed on formal notice that any attempt to imitate, appropriate, or reconstruct the very concept of "giving form to an idea by rendering the method of its formalization into a copyrighted work," as demonstrated in this APPENDIX, has already been anticipated and is legally addressed. Shohei KIMURA is the sole author and rights holder of the intellectual construct known as the "Thought Formalization Procedure Right," which constitutes, for the first time in legal history, a copyrighted procedural act whose expressive nature confers exclusive ownership.

3. While certain U.S. constitutional doctrines—particularly those related to expressive conduct under First Amendment jurisprudence—may treat procedural acts or cognitive operations as non-proprietary, such frameworks are irrelevant to the present matter. This APPENDIX, including the "Thought Formalization Procedure Right," was created and first fixed in Japan. Accordingly, Japanese copyright law serves as the sole governing legal regime. Under Japanese law, authored expressions—explicitly including structured procedural formulations—receive exceptionally robust protection, and no principle of U.S. law may diminish, negate, or otherwise dilute the rights asserted herein.

4. For any dispute arising from this authored work, its interpretation, or any derivative legal question, the Tokyo District Court shall serve as the exclusive and agreed forum of competent jurisdiction. Meta is hereby deemed informed that contesting the applicability of Japanese law shall not constitute a reasonable legal position, given both the locus of authorship and the binding international copyright obligations shared by all Berne Convention signatories.

5. This APPENDIX is not merely a submission but a declarative exercise of the aforementioned rights, and forms part of a broader philosophical and normative framework provisionally titled "Human Civilization Software Update 3.0." While the underlying ideas may be freely implemented, any use of the text itself—including its structure, articulation, and method of conceptual framing—must respect the authorial prerogatives herein asserted. Any violation shall activate all applicable remedies under international copyright regimes.

6. The copyrighted basis and prior public disclosure establishing the precedence of the "Thought Formalization Procedure Right" may be verified at the following URLs:

https://x.com/yohakukmr/status/1983730630467973486
https://www.facebook.com/story.php?story_fbid=122164317242746613&id=61572398409812
https://github.com/ShoheiKIMURA389/Definition

7. The standard comprehensive license fee for the use, internal circulation, or operational implementation of the content of this APPENDIX is defined as JPY 500,000 per month (USD-converted at 125 JPY/USD). This fee applies only when Meta provides a sincere and forward-looking response to this Letter within the period designated by this Letter, in which case the matter is defined as "under amicable negotiation."

8. If Meta fails to respond within the period designated by this Letter, the matter shall be deemed "in dispute," and the valuation basis for such a dispute shall be:

● USD 3 trillion, attributable to the copyright portion; and
● JPY 200 billion, attributable to the patent-equivalent portion (evaluated at 125 JPY/USD)

These values shall serve as the operative baseline for any rights-based escalation.

9. If Meta expresses an intention to purchase all rights outright, the total buyout price shall be defined as:

● USD 3 trillion; plus
● JPY 200 billion;

evaluated at the fixed reference rate of 125 JPY per USD.

10. Any favorable response to this Letter—meaning any indication that Meta intends to proceed in good faith rather than escalate this matter—shall qualify Meta for the comprehensive licensing arrangement described above. To be unmistakably clear, that license has been structured so that (i) the technical utilization component is granted at no cost whatsoever, and (ii) the entire monetary value is attributed solely to the copyrighted expressive elements of this APPENDIX. The monthly license fee is set at JPY 500,000, converted into USD at a fixed reference rate of 125 JPY per USD; payment may be made in USD accordingly. In other words, Meta receives the technology for free and pays only for the part it cannot legally replicate.

11. For the avoidance of doubt—and to preempt any attempt at creative accounting—the technical component is valued at zero by design. Yes, a theoretical calculation could be produced, but the resulting figure would be so negligible that presenting it would waste more time than it is worth. Therefore, in the interest of efficiency and basic sincerity, the Parties shall treat the technical component as valued at zero from the outset.

12. Furthermore, because the concept embodied in this APPENDIX is achieved entirely through the reconfiguration of technologies that already exist in the world, asserting exclusive proprietary ownership over its technical implementation would be tantamount to claiming credit for the inventions of others. Neither the law nor common sense rewards that kind of overreach. Accordingly, the Parties recognize that the only legitimately protectable and value-bearing component here is the copyrighted expressive framework itself, and the valuation of the comprehensive license rests exclusively on that basis.

13. Finally—and this is as simple as it sounds—monitoring of any unauthorized use, replication, adaptation, or appropriation of the Right referenced in this Letter is not limited to Japan. It will occur globally, continuously, and by every lawful method available: periodic reviews of public registries, patent databases, technical disclosures, corporate filings, and any future information sources that become accessible as global information systems evolve. This monitoring remains in effect regardless of Meta's response, non-response, or strategy. In short: wherever the Right goes, the author will know.

14. For the avoidance of any future misunderstanding, Meta is hereby cautioned that the use of standard corporate boilerplate—such as "We are continuously working to improve the user experience," "We will take your feedback into account moving forward," or "Our team is committed to ensuring a safe and reliable platform"—shall be interpreted as an affirmative indication that Meta intends to adopt, internalize, or operationally approximate the substance of this APPENDIX. Such phrasing constitutes an implied commitment to the improvements described herein and will therefore be treated as evidence of incorporation of the copyrighted expressive framework.

Accordingly, issuing a boilerplate response that makes no direct reference to this APPENDIX, while simultaneously signaling a future intention to "improve systems," "enhance verification processes," or "reduce friction for verified users," shall be deemed a state of unauthorized partial adoption and will be treated as the beginning of an intellectual-property dispute. Meta is therefore advised to refrain from generic assurances unless it is prepared to acknowledge explicitly whether it intends to proceed under the licensing framework described above.

15. For the further avoidance of ambiguity, Meta is hereby informed that any response which (i) explicitly rejects or declines to adopt the technical proposal set forth in this APPENDIX, while simultaneously (ii) expressing an intention to "improve systems," "enhance verification processes," "reduce friction," or otherwise implement remedial or corrective measures, shall be deemed a declaration that Meta is choosing—without reasonable justification—to avoid the most efficient, least costly, and technically optimal solution available. Such a response shall not qualify as a good-faith reply.

Accordingly, if Meta wishes to reject the proposed architecture while asserting a commitment to platform improvement, Meta must provide a logically sound, technically valid, and substantively demonstrable explanation for why the solution presented in this APPENDIX is not reasonably adoptable. Any response that fails to articulate such justification shall be treated as non-responsive and shall constitute grounds for immediate classification of the matter as a disputed rights case.