CLEAR ACT
FINANCIAL REBELLION 090326

The CLEAR Act's Guardrails on Programmable Money

The core idea: Programmable money can be coded to freeze, block, restrict, or expire on command. The CLEAR Act doesn't ban programmable money — it puts guardrails around who can pull those levers, when, and with what accountability. *(Section 2)*

Key term — "Controlling person": Most of these guardrails are duties imposed on whoever actually holds the power to freeze, block, or alter your digital money — the issuer, the custodian, the exchange, the smart-contract administrator, or whoever else holds the technical keys. The Act calls this person or entity the "controlling person." It's a functional test, not a title: whoever can pull the lever is on the hook. *(Section 3(a)(2)–(3))*

What this applies to, and how it fits with federal law:

- The broadest duties (disclosure, transparency, non-discrimination) apply to any "covered digital asset" — a wide category including stablecoins, tokenized deposits, tokenized securities, NFTs, and governance tokens. *(Section 3(a)(1))*
- The narrower "programmable money" label — and the specific guarantee that you can always get a non-programmable payment option — applies only to digital assets used as a medium of exchange that carry coded restrictions. *(Section 3(a)(4), Section 21)*
- The Act is built to sit alongside federal law, not override it. It doesn't attempt to regulate the issuance or registration of any instrument, and it explicitly steps back wherever a federal statute or regulation — like the GENIUS Act's federal framework for payment stablecoins — specifically requires something different. *(Sections 8, 9, 24(a))* **Note:** the text itself doesn't name the GENIUS Act — it uses general "federal-compliance" and anti-preemption language designed to avoid conflict with whatever federal stablecoin regime applies. Worth flagging on air as an inference, not a direct textual reference, unless you want me to

draft explicit GENIUS Act coordination language to add to the bill itself.

On AML/KYC — this doesn't eliminate it, it targets over-application of it: Banks and issuers are already required by federal law (the Bank Secrecy Act and related AML/KYC rules) to screen and report suspicious transactions. The Act doesn't try to undo that. What it targets is the tendency of controlling persons to build broad, automated algorithms that catch far more transactions and people than the law actually requires — because over-blocking protects *them* from regulatory penalty, even at your expense. *(Section 7(c), Section 8, Section 16(b))* The guardrail is: comply with what's actually federally required, in the "least restrictive manner" that requirement allows — not the broadest, safest-for-the-bank interpretation of it.

Guardrail 1: You Can't Be Frozen Out for Who You Are or What You Believe *(Section 5)*

- The controlling person is banned from denying, blocking, or restricting your digital money based on: your politics, religion, speech, medical choices (including vaccination status), what you buy or browse, where you live, your job or industry, or any "social credit score"-style rating *(Section 5(a)(1)–(10))*
- The only carve-out: an actual criminal transaction, and even then due process protections apply *(Section 5(b))*

Guardrail 2: You Get to Know Why *(Section 6)*

- If your funds are frozen or your account is restricted, the controlling person must give you a phone number, address, and email to ask why *(Section 6(a)–(b))*
- Within 30 days, they must hand you a written explanation citing the exact rule they used — no vague "policy violation" excuses *(Section 6(c))*

Guardrail 3: No Blanket Freezes — Only Individual, Specific Orders *(Section 7)*

- The controlling person can't freeze your money because of a standing algorithm targeting "categories" of people (an industry, a region, a type of transaction) — this is the guardrail against over-broad AML/KYC-style dragnets described above *(Section 7(c))*

- A freeze requires a particularized order naming you specifically *(Section 7(a)–(b))*
- Exception: narrowly, if federal law specifically and directly requires it, applied in the least restrictive way possible *(Section 8)*

Guardrail 4: Your State Government Needs a Warrant to See Your Transactions *(Section 10(a)–(b))*

> **A note on "government" here:** this Act can only regulate *state* government — this state's own agencies and officials. It legally cannot, and does not attempt to, restrict federal agencies (like the FBI, IRS, or NSA) or another state's government, which operate under their own federal or state law. *(Section 3(a)(10); Section 10(a)–(b))*

- Your state government can't look at your transaction history without a warrant based on probable cause *(Section 10(a))*
- If they do get a warrant, you must be notified within 90 days *(Section 10(b))*

Guardrail 5: The "Data Purchase Loophole" Is Closed *(Section 10(c))*

- State government can't buy its way around the warrant requirement using a data broker

Guardrail 6: No Mass Surveillance Fishing Expeditions *(Section 10(d))*

- State government can't run bulk searches asking "show me everyone who transacted with X" without a warrant tied to a specific crime, narrowly scoped *(Section 10(d), noted as an optional/higher-protection provision)*

Guardrail 7: Controlling Persons Must Protect Your Data by Default *(Section 12)*

- Collect only what's needed, don't sell it, delete it when done, notify you of breaches *(Section 12(a)(1)–(4))*

Guardrail 8: Privacy Tools Are Protected, Not Treated as Suspicious *(Section 13)*

- The controlling person must offer privacy-protective options where feasible *(Section 13(a))*
- Using encryption or self-custody can't, by itself, be treated as "suspicious activity" *(Section 13(b))*

Guardrail 9: The Fine Print Has to Be Public *(Section 14)*

- The controlling person must publicly disclose everything the code can do to you — freeze, expire, reverse, restrict *(Section 14(a))*
- Undisclosed restrictions can't be enforced, and you can be compensated if one is used against you *(Section 14(b)–(c))*

Guardrail 10: Whoever Holds the "Kill Switch" Must Be Named *(Section 15)*

- The controlling person must publicly identify the specific people or key-holders who can alter, freeze, or upgrade the asset *(Section 15(a))*
- 30 days' notice before major changes to that authority *(Section 15(b))*

Guardrail 11: The "Compliance Blocklist" System Is Disclosed (with a Confidential Tier) *(Section 16)*

- Public: that screening happens and who's doing it *(Section 16(a))*
- Confidential, filed with regulators only: the specific criteria and thresholds — this protects legitimate AML screening logic from public gaming while still allowing audit *(Section 16(b)–(d))*

Guardrail 12: You Always Have a Cash/Non-Programmable Option *(Section 21)*

- Large merchants, government agencies, and essential-service providers must offer a non-programmable payment option free of charge *(Section 21(a)–(b))*

Guardrail 13: The State Restrains Itself *(Section 22)*

- State agencies can't impose programmable restrictions on your payments, condition benefits on surveillance, or adopt a CBDC without legislative authorization *(Section 22(a)(1)–(3))*

Guardrail 14: Real Teeth for Enforcement *(Section 25)*

- Attorney General can sue, fine, and force compliance *(Section 25(a))*

- Individuals can sue directly and recover damages plus attorney's fees *(Section 25(b))*
- Evidence gathered in violation of the warrant rule is thrown out of court *(Section 25(f))*