

ANALYSIS REPORT

Tokenization, Sovereign Rights, and Legal Tender in Wisconsin

Analysis of LRB-0372/P1 (UCC 2022 Amendments), the CLEAR Act (full model text), and the CAGE/Cash Act for the 2027–2028 Legislature

Prepared: October 14, 2026

Subject: Compatibility, rights protection, constitutional risk, cash as a buffer, and passage recommendations

Status of source drafts: LRB-0372/P1 is a preliminary draft; CAGE has a placeholder effective date; CLEAR reviewed in full (Solari Model v1.0-Expanded). Version 4 (adds AI-agent definition, accountability, and decision-custody sections).

1. Executive Summary

Bottom line (version 2, incorporating the full CLEAR text). The three drafts still sit on three different layers and remain largely complementary: LRB-0372/P1 (2022 UCC amendments, new ch. 412) supplies commercial-law certainty for digital assets but is rights-neutral; the CLEAR Act supplies the rights overlay; the CAGE Act supplies a physical-cash floor that no code, key, or data feed can switch off.

Recommendation: pass CAGE in whole with technical amendments; pass LRB-0372 in whole with a CLEAR cross-reference and term alignment; and pass CLEAR **in part in 2027** by section: the state-restraint, self-custody, government-access privacy, transparency, and core nondiscrimination provisions now, and the provisions that most directly collide with federal banking, sanctions, and fraud-prevention practice (the standing-rule ban in § 7(c), the all-accounts anti-debanking rule in § 23, the privacy-technology duty in § 13(a), pre-deployment audits in § 17, and the strict-liability remedy structure) revised or deferred to 2028.

What the full text changed.

- **Resolved concerns.** CLEAR § 14(c)(3) already bars cease-and-desist relief against a transferee for value without notice (compensation is the exclusive remedy), which largely reconciles CLEAR with the UCC take-free rule. CLEAR § 22(a)(3) already bars state agencies from participating in a CBDC absent express legislative authorization, which settles the CBDC policy question without changing the UCC. CLEAR § 22(b) covers state disbursements, and § 25(c) supplies an enforcement route against state agencies, filling two gaps I had identified in CAGE.

- **New concerns.** (1) The introduction says CLEAR includes a fraud-prevention exception; the text does not. Section 8 excuses only actions *specifically required* by an identified federal statute, regulation, or order, and § 7(c) bars standing automated rules based on categories of conduct, geography, industry, or transaction type. Read literally, that reaches ordinary fraud screening, velocity limits, and risk-based holds. (2) Section 23 extends anti-debanking and due-process rules to depository institutions' account and payment services generally, not only tokenized assets, and § 24(b) states the duties are enforceable against national banks, inviting a preemption fight. (3) Liability is strict (§ 25(i)), with statutory damages, fair-market-value compensation, attorney's fees, and discretionary punitive damages of up to three times actual damages. (4) Section 13(a) imposes a duty to offer privacy-protective options (including mixing techniques under the § 3(11) definition). (5) Section 11 purports to define a reasonable expectation of privacy "for purposes of the constitution," which a legislature cannot do. (6) Several model-act placeholders do not fit Wisconsin institutions (Section 8.6).
- **Rights.** Only CLEAR, and narrowly CAGE, directly protect individual rights. The UCC upholds property and contract expectations among private parties and is neutral on programmable controls, surveillance, and compelled payment methods.
- **AI agents.** CLEAR § 3(3) defers the question of who is the controlling person when an AI agent exercises technical control to "applicable state law," and Wisconsin has no clear rule. Section 9 recommends defining an AI agent as a tool, not a legal person, attributing its acts to accountable persons (deployers and those holding administrative authority), requiring disclosure and decision custody records (with presumptions when records are missing), treating agent-held keys as the deployer's, and keeping CLEAR civil-only.
- **Cash as buffer.** A state statute requiring government acceptance of U.S. coin and currency remains the lowest-risk, highest-certainty instrument in the set. CLEAR § 22 and § 21 reinforce it but are weaker for state agencies, because they permit a non-programmable *electronic* alternative where CAGE requires cash.
- **Federal and industry risk.** UCC and CAGE: low. CLEAR's state-restraint, self-custody, government-access, and transparency provisions: low to moderate. CLEAR's private-sector control rules (§§ 7(c), 12, 13(a), 17, 23, 24(b)) reach into BSA/OFAC practice, the GENIUS Act's issuer freeze obligations, and National Bank Act and Federal Credit Union Act preemption, and draw the strongest banking, credit union, and national-security resistance.

2. Scope, Sources, and Current Federal Context

2.1 Documents reviewed

Draft	What was reviewed	Notes
LRB-0372/P1	Full 106-page Legislative Reference Bureau preliminary draft (2027–2028 Legislature), adopting the Uniform Law Commission's 2022 UCC amendments	Marked "Preliminary draft – not ready for introduction"; no sponsor. Creates ch. 412 (controllable electronic records) and amends chs. 401–411 and other statutes. Takes effect on the first day of the 4th month after publication; transition "adjustment date" about one year later or July 1, 2029, whichever is later.

Draft	What was reviewed	Notes
CAGE Act, draft B4F	Full text, 9 sections	Effective date is a placeholder ([DATE]). No enforcement or remedy section.
CLEAR Act (Solari Model Legislation v1.0-Expanded)	Full 15-page model text, 29 sections in six Parts, plus the earlier one-page legislator introduction (Oct. 6, 2026)	Privately sponsored model act with bracketed placeholders. The introduction's four "parts" correspond to bill Parts II–V; Part I is definitions and Part VI is coordination, enforcement, and general provisions. This report cites the bill's own section numbers.

2.2 Federal and market context as of October 11, 2026

- **GENIUS Act (payment stablecoins).** Signed July 18, 2025. Takes effect on the earlier of January 18, 2027 or 120 days after final implementing rules. Regulators missed the July 18, 2026 rulemaking deadline; final rules (OCC, Treasury, FinCEN/OFAC) were still pending in recent reporting, so January 18, 2027 is the likely operative date. Federal law requires issuers to be able to comply with lawful orders, which matters for CLEAR §§ 7 and 8.
- **Market-structure legislation.** The CLARITY Act was reported to have stalled in August 2026, leaving federal treatment of developers, self-custody, and peer-to-peer payments unsettled.
- **CBDC.** Executive Order 14178 (Jan. 2025) bars federal agencies from establishing or promoting a CBDC. The Anti-CBDC Surveillance State Act has passed the House and, per available reporting, is pending in the Senate (final enactment unconfirmed; verify).
- **UCC adoption.** The 2022 UCC amendments had been enacted in 33 states as of the end of 2025.
- **Wisconsin political calendar.** The governor and half the State Senate are on the November 3, 2026 ballot. I do not assume an outcome. 2027 will be dominated by the 2027–29 biennial budget.

2.3 What changed from the first version of this report

Issue	Version 1 (introduction only)	Version 2 (full CLEAR text)
Take-free vs. CLEAR remedies	Flagged as a friction requiring a UCC amendment	Largely resolved by CLEAR § 14(c)(3). Remaining gaps: § 14(c)(3) protects only transferees for value without notice (not "qualifying purchasers" as defined in § 412.102(1)(b)), and it governs § 14 remedies only, not the general § 25(b) remedies.
CBDC policy	Recommended a standalone statute (Option A)	CLEAR § 22(a)(3) is that statute. Option A is confirmed; no UCC change needed.
CAGE gaps	No enforcement; no disbursements	CLEAR § 25(c) and § 22(b) supply models for both.
Fraud-prevention exception	Assumed present, per the introduction	Not in the text. Only § 8 (federal compliance, "specifically required") and § 5(b) (criminal offenses). A material gap.
Scope of due-process rules	Assumed limited to tokenized assets	§ 23 reaches depository institutions' accounts and payment services generally; § 7(c) bans standing automated rules.
Constitutional language	Not visible	§ 11 and § 25(f) declare privacy expectations "for purposes of the constitution" and create a statutory suppression rule; both need Wisconsin-specific review.

Issue	Version 1 (introduction only)	Version 2 (full CLEAR text)
CLEAR recommendation	Pass in part by Part	Pass in part by section (Section 8.5), with amendments.

3. Part One: Compatibility and Incompatibility

3.1 The three bills sit on different layers

Layer	Bill	Function	Relationship to tokenization
Property and commercial law	LRB-0372/P1 (UCC 2022)	Defines "control" of digital assets, perfection and priority of security interests, take-free rules, choice of law, and "electronic money"	Gives tokenized assets legal certainty. Technology-neutral and expressly not a regulatory or rights statute.
Individual rights overlay	CLEAR Act	Nondiscrimination and due process (Part II), financial data privacy (III), code and control transparency (IV), financial freedom and state operations (V), enforcement (VI)	Constrains how tokenized assets may be controlled, surveilled, and imposed on residents. Self-contained definitions ("covered digital asset," "technical control," "controlling person") that do not depend on the UCC.
Payment-access floor	CAGE Act	Requires government entities and their payment-collecting contractors to accept U.S. cash	Ensures a non-digital path to discharge obligations to government however other assets are tokenized.

3.2 Pairwise compatibility matrix

Pair	Where they fit	Where they conflict or leave gaps	Suggested fix
UCC + CLEAR	UCC § 412.103(2) subjects ch. 412 transactions to any rule of law establishing a different rule for consumers. CLEAR § 14(b) makes disclosed code a binding term, consistent with the UCC's reliance on terms "readily available for review" (§ 412.107(3)). CLEAR § 14(c)(3) protects transferees for value without notice, mirroring § 412.104(5) and (7). CLEAR § 3(1) covers tokenized deposits and securities that ch. 412 excludes from "controllable electronic record."	(1) "Control" (UCC) and "technical control" (CLEAR § 3(2)) are different concepts; one token can have a UCC controller (the holder) and a CLEAR controlling person (the issuer). (2) § 14(c)(3) uses a looser transferee test than "qualifying purchaser," and does not limit the general § 25(b) remedies. (3) § 7(c) can be read to reach automated liquidations, escrow, vesting, and other consensual code features that Article 9 and ch. 412 expressly accommodate (§ 412.105(2)(a)).	Add a CLEAR cross-reference/savings clause in ch. 412; define "technical control" as distinct from ch. 412 and 409 "control"; use "qualifying purchaser" in CLEAR and apply the transferee protection to all § 25 remedies; add a holder-elected and disclosed-contract-terms exception to § 7(c).
UCC + CAGE	CAGE "cash" corresponds to the UCC's new "tangible money" (§ 409.102(1)(th)), perfected by possession.	No substantive conflict. CAGE does not cross-reference the UCC terms, and the UCC creates "electronic money" (potentially including a future CBDC).	Cross-reference "tangible money" in CAGE and state that electronic money, stablecoins, deposits, and tokenized cash-equivalents are not "cash."

Pair	Where they fit	Where they conflict or leave gaps	Suggested fix
CLEAR + CAGE	Both bar state agencies from forcing a payment method. CLEAR § 22(a)(2) bars conditioning any benefit, license, permit, or service on use of a particular payment instrument; § 22(b) requires state payments to residents in non-programmable form on request. CAGE § 4(d) bars exclusive electronic payment and § 5 reaches contractors; CLEAR defines "state agency" to include contractors.	CAGE is stricter on cash: CLEAR § 21(b) lets an agency that requires programmable money satisfy the duty with any non-programmable electronic option (§ 3(20)), which is not cash. Different defined terms ("governmental entity" in CAGE; "governmental entity" and "state agency" in CLEAR §§ 3(10), 3(17)). CAGE has no remedy; CLEAR § 25(c) does.	Make cash acceptance under CAGE the floor and state so in CLEAR § 21; use one defined term; apply CLEAR § 25(c) enforcement to CAGE; keep CLEAR § 22(b) for disbursements.
All three	Layered stack: UCC gives legal certainty, CLEAR protects the holder, CAGE protects the payer to government.	Sequencing risk: UCC alone legitimizes programmable-control assets with no rights overlay.	Enact together, or enact the UCC with the savings clause and at least CLEAR §§ 14–16, 18–20, and 22 in the same session.

3.3 Detailed points of friction and fit

1. **Two different "control" concepts (UCC § 412.105; CLEAR § 3(2)).** The UCC treats a person as having exclusive control even if the system limits use or has a protocol programmed to cause a change, including a transfer or loss of control (§ 412.105(2)(a); § 409.1055(2)(a) for electronic money). CLEAR defines "technical control" as anyone's ability to create, block, freeze, restrict, condition, expire, reverse, burn, or alter an asset, and regulates those persons. These operate on different questions (who owns and can pledge versus who may exercise a control and how), so they coexist, but the shared vocabulary invites confusion. The two statutes should say expressly that a person can be the holder with "control" under ch. 412 and a third party can be a "controlling person" under CLEAR.
2. **Take-free finality vs. CLEAR remedies.** A qualifying purchaser takes free of competing property claims, and no conversion, replevin, constructive-trust, or equitable-lien action lies against it (§ 412.104(5),(7)). CLEAR § 14(c)(3) correctly directs that cease-and-desist relief not run against a transferee for value without notice, with damages as the exclusive remedy. Two refinements: use the UCC's "qualifying purchaser" (control, value, good faith, no notice) so the tests do not diverge, and extend the protection to remedies under §§ 5–7 and 25(b), because as drafted it appears only in the § 14 remedy provision.
3. **Choice of law is mostly a non-conflict.** UCC § 412.107 selects the law governing property matters covered by ch. 412 (record-designated jurisdiction, then system rules, then the District of Columbia). CLEAR is consumer-protection law tied to Wisconsin residents and state agencies (§ 27 nexus; § 25(l) deemed purposeful availment). The UCC's consumer carve-in (§ 412.103(2)) supports this. A short statement that CLEAR is a non-waivable rule applying regardless of a CER's chosen jurisdiction would remove residual doubt.
4. **Standing-rule ban (CLEAR § 7(c)) vs. Article 9 and ordinary token mechanics.** Section 7(c) bars standing, automated, algorithmic, or code-based rules that block, freeze, expire, restrict, or terminate a resident's covered digital asset based on general categories of conduct, geography, industry, or transaction type, absent a particularized order or the narrow federal-compliance

exception. Article 9 secured-party control and enforcement (new §§ 409.1055, 409.1072, 409.208(2)(g)), escrows, vesting schedules, time-locks, collateral-ratio liquidations, holder-configured spending limits and allowlists, parental controls, and ordinary fraud holds are all code-based restrictions. Only § 9 (securities) is carved out. A holder-elected and advance-disclosed contract-terms exception, plus a fraud and unauthorized-transaction exception, are needed.

5. **Deposits and real estate.** Ch. 412 excludes deposit accounts, electronic money, investment property, and transferable records from "controllable electronic record" (§ 412.102(1)(a)), and Article 9 does not govern land. CLEAR § 3(1) covers any token recorded on a distributed ledger over which any person holds technical control, expressly including tokenized deposits, tokenized securities, and CBDC, so its protections attach regardless of how the UCC classifies the asset. For real estate, CLEAR reaches the token and its controls but not the formalities of conveyance and recording (Wis. Stat. ch. 706); a separate title and recording statute remains a gap.
6. **Electronic money and CBDC.** The UCC would define electronic money as government-authorized money in electronic form, including any future CBDC, while excluding cryptocurrency predating government adoption. That recognition authorizes nothing. CLEAR § 22(a)(3) provides that no state agency shall adopt, require, accept, or participate in a CBDC arrangement without express legislative authorization. Keeping the UCC uniform and handling CBDC through CLEAR § 22 (Option A, Section 8.4) is the cleanest structure. If CLEAR does not pass, an equivalent stand-alone provision should accompany the UCC.
7. **Federal overlay.** The UCC bill states that it does not address regulation, taxation, or securities status. CLEAR's federal-compliance exception (§ 8) is narrower than the introduction suggests (see Section 7.1), and the GENIUS Act's freeze-and-comply obligations for issuers are the most likely point of collision.

3.4 Outcomes under different combinations

Combination	Likely outcome	Principal residual risk
UCC only	Wisconsin law recognizes and finalizes digital-asset transactions and secured lending. Rights-neutral.	Programmable controls, surveillance, and mandated digital payment are legally recognized but unaddressed. No state-level buffer.
CAGE only	Physical-cash path for payments to government.	Does not reach private tokenized assets, data privacy, or freeze/due-process risk. Wisconsin commercial law lags peers.
CLEAR only	Self-contained rights overlay with its own definitions; operable without the UCC.	Remedy and transferee rules sit outside UCC take-free rules, risking mismatch; carries the full regulatory load and therefore the full preemption exposure.
UCC + CAGE	Modern plumbing plus a cash floor.	Holder-side risks (freeze, surveillance, disclosure) remain.
UCC + CLEAR (no CAGE)	Modern plumbing plus holder rights and state self-restraint.	CLEAR § 21 permits a non-programmable electronic alternative rather than cash, so no guaranteed cash floor.
UCC + CAGE + CLEAR (partial), recommended	Layered stack with the least contestable CLEAR provisions first.	Deferred CLEAR provisions remain for a later session.

4. Part Two: How Each Bill Upholds Sovereign and Constitutional Rights

4.1 Rights framework

"Human sovereign rights" are mapped here to the enforceable constitutional guarantees that most directly bear on money and property. A threshold point: the federal Bill of Rights restrains government, not private issuers. Rights risk arises in tokenized finance through four pathways: (a) the government is itself the issuer or operator (e.g., a CBDC or a state-issued token); (b) government directs, coerces, or encourages private intermediaries to restrict or surveil (state-action doctrine; see *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989); *NRA v. Vullo*, 602 U.S. 175 (2024)); (c) government obtains transaction data from private custodians (*Carpenter v. United States*, 585 U.S. 296 (2018), limits but has not abolished the third-party doctrine of *United States v. Miller*, 425 U.S. 435 (1976)); and (d) state law gives legal force to code-based deprivations. Statutes like CLEAR matter precisely because they create statutory rights against private actors where constitutional doctrine may not reach.

Interest	Federal anchor	Wisconsin anchor	Tokenization risk vector
Property / no deprivation without process	5th and 14th Amendments (due process; takings); <i>Fuentes v. Shevin</i> , 407 U.S. 67 (1972); <i>Mathews v. Eldridge</i> , 424 U.S. 319 (1976)	Wis. Const. art. I, § 1 (inherent rights; the source of civil due process), § 13 (takings), § 8 (criminal process)	Automated freeze, expiry, or forced transfer with no human review or notice
Privacy / unreasonable searches	4th Amendment; <i>Carpenter</i> ; Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. (federal access only)	Wis. Const. art. I, § 11; existing warrant statutes for electronic and location data (e.g., Wis. Stat. §§ 968.373, 968.375, as analogues; verify)	Public-ledger transaction graphs; data purchase from brokers; privacy-tool restrictions
Speech, association, religion, equal treatment	1st and 14th Amendments; <i>Vullo</i>	Wis. Const. art. I, §§ 1, 3, 4, 18	Controls conditioned on lawful political, religious, or associational activity; social-credit-style scoring
Monetary sovereignty / legal tender	U.S. Const. art. I, § 8, cl. 5; art. I, § 10, cl. 1; 31 U.S.C. § 5103	Legislature's authority over its own agencies and contracts	Forced use of digital or programmable money for public payments
Federalism / state non-participation	10th Amendment anti-commandeering (<i>Printz v. United States</i> , 521 U.S. 898 (1997); <i>Murphy v. NCAA</i> , 584 U.S. 453 (2018))	State may decline to use its own agencies to implement federal programs	A federal CBDC or ledger mandate could not compel state agencies to implement it, but state law should say so

4.2 CAGE Act

Rights upheld.

- **Monetary/legal-tender sovereignty.** Section 4 requires every state and local governmental entity, and every public institution of higher education, to accept U.S. coin and currency for any fee, fine, tax, assessment, charge, admission, fare, toll, or other obligation. This operationalizes, at the state

level, the federal rule that U.S. coins and currency are legal tender for "all debts, public charges, taxes, and dues" (31 U.S.C. § 5103).

- **Equal access and nondiscrimination.** Section 4(d) bars making any credit card, debit card, EFT, mobile app, or digital wallet the exclusive means of payment; § 4(e) bars cash surcharges. Residents are not required to hold a bank account or a device, which protects the unbanked, rural, elderly, and privacy-conscious from exclusion from government services.
- **Privacy.** The findings (§ 2(c)) tie cash acceptance to "individual privacy" and freedom to transact lawfully without reliance on digital systems. A cash payment to government generates no third-party ledger entry.
- **Anti-circumvention.** Sections 5 and 6 reach private contractors collecting public payments and bar delegating collection to evade the Act, closing the most obvious outsourcing loophole.

Risk if assets are tokenized without CAGE. A state or local entity could move to cashless collection (e.g., a tokenized-deposit or stablecoin-only portal for permits, fines, tuition, transit fares, or court costs), making enrollment with a regulated intermediary, identity verification, and data disclosure preconditions of access to public services. Where the intermediary applies automated screening or controls, the resident's ability to pay a fine or tax could itself be switched off, producing due-process and equal-protection problems that are hard to litigate after the fact.

Gaps to close (see Section 8.3). No enforcement mechanism (CLEAR § 25(c) offers a model); no coverage of disbursements to individuals (CLEAR § 22(b) covers state payments to residents); "cash" is not cross-referenced to UCC "tangible money"; no express treatment of unattended/automated collection points; no data-minimization rule for cash payment records; the phrase "subject to applicable federal law" in § 4(a) is open-ended; effective date unset.

4.3 CLEAR Act (full text, Parts II–V and enforcement)

Bill part and sections	Rights upheld	Risk if tokenized without it	Drafting observations
Part II, §§ 5–9: nondiscrimination, statement of reasons, lawful-order due process, federal-compliance exception, securities carve-out	Equal treatment and association (1st/14th Amendments; Wis. Const. art. I, §§ 1, 3, 4, 18) by barring controls based on listed factors (including political, religious, and other lawful opinions, location, trade, any lawful activity, and social-credit scoring). Procedural due process (<i>Fuentes</i> , <i>Mathews</i>): written reasons within 30 days (§ 6), particularized orders and prompt notice (§ 7(a),(b)).	Automated, unreviewable freezes or expiry; blocking for lawful but disfavored activity; no human recourse; government pressure on intermediaries to implement controls invisibly to the holder (<i>Vullo</i>).	Strongest rights provisions and the most contestable. "Any lawful activity" and "geographic location" are very broad factors. § 7(c) bans standing automated rules. § 8 excuses only actions "specifically required" by an identified federal statute, regulation, or order, applied in the least restrictive way, with the controlling person bearing the burden. No fraud-prevention exception appears in the text.

Bill part and sections	Rights upheld	Risk if tokenized without it	Drafting observations
Part III, §§ 10–13: government access to ledger data, privacy declaration, private data duties, privacy-enhancing technology	4th Amendment and Wis. Const. art. I, § 11 interests: warrant on probable cause for Wisconsin state and local access to transaction-graph data (§ 10(a)), 90-day notice (§ 10(b)), ban on buying ledger-analytics data (§ 10(c)), optional ban on bulk or reverse searches (§ 10(d)), statutory suppression (§ 25(f)). Private data minimization and no-sale duties (§ 12). Safe harbor for lawful use of privacy-enhancing tools (§ 13(b)).	Public-ledger transaction graphs become permanent searchable records; the third-party doctrine and data-broker purchases can then be used to avoid a warrant; privacy tools treated as suspicious.	§ 10 expressly governs only Wisconsin governmental entities and does not limit federal process, which keeps it low-risk federally. It excludes administrative subpoenas, which affects civil and regulatory agencies. § 11 declares expectations of privacy "for purposes of the constitution," which courts, not legislatures, decide. § 13(a) imposes an affirmative duty to offer privacy options, where not prohibited by statute, with a private right of action.
Part IV, §§ 14–18: disclosure of code, keys, oracles; assurance; immutable deployments	Notice and informed consent as preconditions to due process: public, plain-language, machine-readable disclosure of material terms and any freeze, reverse, expire, or burn capability, treated as a binding term (§ 14); identity and scope of admin and upgrade key holders with 30-day upgrade notice (§ 15); public identification of oracle and compliance-data providers with confidential filing of screening logic (§ 16); immutable and ownerless deployments excluded (§ 18).	Hidden freeze or blacklist functions, upgradeable-proxy admin keys, unseen compliance feeds with no human in the loop; terms of service that disclaim the controls that actually operate.	Function-based and technology-neutral, and the tiered confidentiality in § 16 and the exception for SAR-confidential information are well designed. Concerns: strict liability and damages (§§ 14(c), 25(i)); public identification of natural-person key holders (§ 15(a)(1)); pre-deployment independent examination for non-bank controlling persons (§ 17(a)); officer certification to the Attorney General for insured depository institutions (§ 17(b)).
Part V, §§ 19–23: self-custody and P2P, validation, non-programmable payment guarantee, state self-restraint, anti-debanking	Liberty and property: right to self-custody and peer-to-peer transacting, with no state licensing or penalty (§ 19); right to validate (§ 20); free non-programmable payment option from merchants above [\$5,000,000] revenue, state agencies, and essential-service billers that require programmable money (§ 21); state agencies may not impose programmable restrictions, condition services on surveillance consent or a particular instrument, or participate in a CBDC without express authorization, and must pay residents in non-programmable form on request (§ 22); anti-debanking for depository institutions, money transmitters, and custodians (§ 23).	State or state-contracted payment systems that condition access on a programmable instrument; indirect pressure toward custodial-only holding; account termination used to cut off access to the ledger economy.	§§ 19–20 and 22 regulate the state itself, the strongest legal footing. § 21's private mandate is conditional ("a person that requires" programmable money). § 23 applies to depository institutions' account and payment services generally, not only tokenized assets. § 19 changes Wisconsin licensing treatment of self-custody software and should be checked against ch. 217.
Part VI, §§ 24–29: coordination, enforcement, nexus, severability	Rights made enforceable: Attorney General enforcement under the state UDAP statute, a private right of action with fees and, for willful or repeated violations, punitive damages up to three times actual damages, mandamus and injunctive relief against state agencies, suppression, and a deemed-jurisdiction rule (§ 25).	Rights without remedies; arbitration and class waivers defeating private enforcement.	Strict liability (§ 25(i)); possible conflict with Wisconsin's punitive-damages cap; revocation of the right to do business assigned to a "Secretary of State" (§ 25(h)); strong severability and independent-operation clauses (§ 28), which protect the remainder of the Act if one part falls. § 24(b) states the duties are enforceable against national banks.

Technical note on extensibility. CLEAR's central definitions are capability-based. "Technical control" (§ 3(2)) is defined by what a person can do (create, block, freeze, restrict, condition, expire, reverse, burn, alter) and by the means used (code, administrative or upgrade authority, oracle or compliance-data input, ledger permissioning, custody), and "covered digital asset" (§ 3(1)) covers any token on any distributed ledger, public or permissioned, over which someone holds technical control. That reaches ERC-20-style freeze and blacklist functions, permissioned-token identity registries and forced-transfer controllers, upgradeable proxies, MPC and multisig custody, account-abstraction keys, and oracle-driven geofencing or expiry without naming any of them, so it should age well. Two drafting questions: whether protocol-level validators and miners that can censor transactions are "controlling persons" (§ 20 protects the right to validate, but does not say validators are outside Part II), and how § 3(3)'s rule for AI agents ("determined by applicable state law") will work in practice.

4.4 LRB-0372/P1 (UCC 2022 amendments)

Rights upheld (indirectly).

- **Property and contract certainty.** Defines control, perfection, priority, and take-free rules so that digital-asset holders and purchasers have enforceable property-type rights in court, and recognizes electronic signatures and records.
- **Consumer carve-in.** Section 412.103(2) subjects Chapter 412 transactions to consumer-specific rules and to Wisconsin's consumer chapters (chs. 421–427, 429 and others listed), and § 412.106 preserves different rules for individual account debtors on personal, family, or household obligations.
- **Protections for innocent purchasers.** Take-free rules and the good-faith definition ("honesty in fact and the observance of reasonable commercial standards of fair dealing") reduce the risk that a buyer's token is clawed back for reasons the buyer could not discover.
- **Security-procedure clarity.** Funds-transfer security procedures may include biometrics and symbols but not merely verifying an e-mail address, IP address, or phone number, a small but real consumer-protective clarification.

What it does not do. It does not limit issuer or controller freezes, does not require disclosure of administrative keys, does not restrict government access to ledger data, does not bar mandated use of any payment instrument, and, by treating programmed loss of control as consistent with exclusive control, gives such features commercial recognition.

Risk if assets are tokenized with the UCC alone. The state would have modernized the law for transferring and financing tokenized assets without any statutory protection for the individual holder against automated or coerced restriction, surveillance, or compelled use. In practice, the lender or counterparty gains stronger rights, while the retail holder's recourse remains whatever the issuer's terms and general federal consumer law provide.

5. Part Three: Constitutional-Rights Risks by Asset Class if Tokenized Without These Revisions

The table below describes risk scenarios, not predictions. Severity depends on who operates the system (government vs. private) and on federal law, which in several areas (BSA/AML, OFAC, GENIUS Act freeze capability, securities law) deliberately requires some control features. Where federal law requires a control, Wisconsin cannot remove it; the objective is process, transparency, and non-discrimination around the control.

Asset class	Tokenized form	Rights at risk	Risk scenario without revisions	Mitigation in the drafts
Money via CBDC	Retail or wholesale central-bank liability on a ledger, potentially programmable	4th (pervasive transaction record); 5th/14th (programmed limits, expiry, caps); 1st (conditions on use); art. I, §§ 1, 11 Wis. Const.	Government is the ledger operator, so state action is direct. Programmable spending limits, expiry, or purpose restrictions; transaction-level visibility; no cash alternative if cash is withdrawn from circulation. Currently low-probability (EO 14178; Anti-CBDC bill pending in Senate) but high-severity and reversible by statute.	CLEAR § 22(a)(1),(3) (state agencies may not impose programmable restrictions or participate in a CBDC without express authorization); CAGE (cash for state and local payments); CLEAR § 10 (warrant). UCC alone would recognize CBDC as "electronic money" without restriction.
Money via stablecoins	Fiat-backed payment tokens (GENIUS Act "payment stablecoins")	14th and 1st (private blacklisting at government direction: <i>Vullo</i>); 4th (issuer and exchange data); property (frozen balances)	Issuers must have technical capability to freeze and to comply with lawful orders; issuer freezes without notice, human review, or reasons; address-level surveillance on public chains; reliance on compliance-data feeds that mislabel addresses; government jawboning of issuers.	CLEAR §§ 5–8 (nondiscrimination, particularized orders, narrow federal exception), §§ 10 and 13 (privacy), §§ 14–16 (disclosure of admin keys and feeds). Federal contestability is highest here.
Stocks	Tokenized equity or tokenized claims on securities held by intermediaries	Property (5th/14th); 4th (investor identity on-chain); 1st (association/shareholder-speech pressure)	Issuer or transfer-agent forced-transfer functions; permissioned-token identity registries sharing holder data; sanctions or compliance feeds triggering automated restrictions; confusion about whether the token is the security or a derivative claim.	UCC: investment-property rules in Art. 8 unchanged for security entitlements; ch. 412 says a CER is not a "financial asset" unless the intermediary agrees. CLEAR §§ 5, 7 and 14–16 for control transparency (§ 9 carves out securities-law transfer restrictions). Securities regulation remains federal.
Bonds (corporate, Treasury, municipal)	Tokenized debt, tokenized Treasuries/money-market funds, on-chain municipal bonds	Property; 14th (procedural due process before restriction); 4th (holder registry); contract rights	Programmatic coupon/transfer restrictions; holder-registry disclosure to compliance vendors; state or local issuers using programmable tokens for their own debt, which implicates art. I § 1 interests and public-finance transparency.	CLEAR §§ 14–16 and 22 (disclosure; state-agency restraint); UCC Art. 8/9 changes for control and perfection. State-issued debt tokenization should be an explicit policy choice.

Asset class	Tokenized form	Rights at risk	Risk scenario without revisions	Mitigation in the drafts
Bank deposits	Tokenized deposits (a deposit-account claim represented by a token on a permissioned ledger)	Property (14th; Wis. Const. art. I §§ 1, 13 if state action); 4th (bank-customer records, <i>Miller</i> limits); ability to withdraw cash	A bank can build programmable restrictions, expiry, geofencing, or purpose limits into deposit tokens; the deposit stays a "deposit account" outside ch. 412, so UCC take-free and control rules do not apply and the customer relies on bank terms and federal law; reduced practical ability to withdraw cash if branches and ATMs shrink.	CLEAR § 3(1) expressly covers tokenized deposits, and §§ 5–7, 14, and 23 apply to them; CAGE (cash for public payments) as a systemic backstop. National Bank Act and FCUA preemption is a major contestability factor (Section 7).
Real estate	Tokenized fractional interests, tokenized deeds or title records, on-chain mortgage notes	Property and takings (5th/14th; Wis. Const. art. I § 13); due process in recording and transfer; 4th (ownership graphs); homestead and equity interests (<i>Tyler v. Hennepin County</i> , 598 U.S. 631 (2023))	Land interests are not within ch. 412 and are governed by ch. 706 and recording law. A token that purports to be the title could be frozen, forfeited, or transferred by code or admin key without the formalities Wisconsin requires; public-ledger publication of ownership; a county or title agency adopting a single vendor's permissioned ledger as the legal record.	UCC does not solve this: fractional-ownership tokens are likely securities (federal law), and conveyance rules are separate. CLEAR § 3(1) reaches tokenized real-estate interests as covered digital assets, and § 22 restrains state and local agencies. A future title/recording statute should require that on-chain controls cannot override ch. 706 formalities.

5.1 Technical drivers of the risk

- **Administrative and upgrade keys.** A token's behavior can be changed by whoever controls an upgradeable proxy or admin role; holders may not know who that is.
- **Built-in freeze/blacklist/forced-transfer functions.** Common in regulated stablecoins and permissioned security tokens; they are lawful and sometimes required, but they are the mechanism through which due-process and discrimination risks materialize.
- **Oracles and compliance-data feeds.** Automated screening depends on third-party data whose errors propagate with no human in the loop; this is the "no human-in-the-loop" problem the CLEAR introduction identifies.
- **Transparent ledgers.** On public chains, address clustering and chain analytics de-anonymize individuals; on permissioned chains the operator sees everything. Privacy-enhancing technologies (zero-knowledge proofs, selective disclosure, stealth addresses, confidential transactions) can reduce exposure but sit in tension with federal AML policy; note *Van Loon v. Department of the Treasury* (5th Cir. 2024), holding immutable smart contracts were not "property" subject to IEEPA sanctions, and subsequent Treasury delisting of the contracts at issue (verify current status).
- **Programmability itself.** Expiry (demurrage), geofencing, spending categories, and conditional release are features a government or issuer can switch on. The harm is not the capability but its use without notice, process, or a non-programmable alternative.

6. Part Four: Cash Acceptance as a Buffer Against Coerced or Forced Digital Payment

A state law requiring government entities to accept cash functions as a structural buffer because it removes the state's ability to make an intermediary, a device, an identity credential, or a programmable instrument a precondition for discharging a public obligation. In summary:

8. **It is anchored in federal law.** U.S. coins and currency are legal tender for "all debts, public charges, taxes, and dues" (31 U.S.C. § 5103). A state statute requiring state and local governments to honor that rule does not make anything a tender in private debts, so it does not implicate the Art. I, § 10 limit on state tender laws; it governs the state's own acceptance of federal tender.
9. **It gives residents a non-digital, bearer, offline payment path.** Cash settles by delivery, needs no account, cannot be frozen by a third party, carries no embedded code, and creates no ledger. For taxes, fines, tuition, fees, fares, and tolls, the resident can always discharge the obligation.
10. **It prevents conditioning access on digital enrollment.** Without cash acceptance, an agency or contractor could require a specific wallet, bank relationship, stablecoin, or (in a future scenario) CBDC account to renew a license, pay a fine, or enroll a child in a public school or university. CAGE § 4(d) and § 6 prohibit that for the asset classes in this report.
11. **It reduces the leverage of automated controls.** A freeze, expiry, or geofence on a tokenized asset is much less coercive if the resident can still pay the state in cash. Cash therefore sets a ceiling on the harm of any programmable instrument in the public-payment context.
12. **It protects privacy at the point of payment.** A cash payment generates no third-party record, which limits the data that could later be reached by subpoena, purchase, or breach.
13. **It preserves state-federal federalism options.** If a federal CBDC or ledger-based payment mandate were ever adopted, a cash-acceptance statute plus CLEAR § 22(a)(3) would give Wisconsin a clear legal basis for refusing to route state functions through it, consistent with anti-commandeering principles.
14. **It is technology-stable.** Because "cash" is defined as physical U.S. coin and currency, the buffer does not depend on predicting what tokenization will look like in five or ten years.

Limits of the buffer (honest scope).

- It covers payments to government and government contractors. It does not by itself reach private merchants, employers, landlords, utilities, or private banks, so it is a floor for civic life rather than a general right to transact in cash.
- It protects only as far as residents can obtain cash. If tokenized deposits or branch closures reduce access to cash withdrawals, the buffer erodes. A complementary right to withdraw deposits in cash (subject to federal law) would strengthen it and is not in any of the three drafts.
- CAGE does not cover disbursements from government to individuals (benefits, refunds, public-employee wages), where a forced digital instrument could also be imposed; CLEAR § 22(b) fills this for state payments to residents.
- It does not prevent the state from offering digital options; CAGE § 7(c) expressly allows them so long as cash remains available. That is the right balance and also makes the bill politically easier.

- CAGE has no enforcement mechanism as drafted; CLEAR § 25(c) (declaratory, injunctive, or mandamus relief against the responsible state agency) is a ready model.

7. Federal Contestability and Industry Pushback

7.1 Federal-law risk of contest, by bill and provision

Risk is rated Low / Moderate / High for the likelihood that a federal agency, a regulated industry, or a private plaintiff could credibly challenge the provision on preemption, intergovernmental-immunity, extraterritoriality, or First Amendment grounds, or that federal law would render it ineffective.

Bill / provision	Federal law implicated	Risk	Why, and how to reduce it
UCC (LRB-0372/P1)	E-SIGN (15 U.S.C. § 7001 et seq., incl. § 7021); securities and commodities law; BSA; GENIUS Act definitions	Low	Uniform commercial law is core state territory; 33 states had adopted by end-2025; the bill disclaims regulation, taxation, and securities status. Keep it technology-neutral and add no regulatory language.
CLEAR §§ 5–6 (nondiscrimination; statement of reasons)	BSA/AML; OFAC and IEEPA; National Bank Act and FCUA preemption (12 U.S.C. § 25b; <i>Cantero v. Bank of America</i> , 602 U.S. 205 (2024)); GENIUS Act	Moderate	Aligns with the 2025 federal fair-banking executive order and <i>Vullo</i> . The factor list is very broad ("any lawful activity," location, trade). Risk-based decisions and federally required geographic restrictions are not clearly excepted. Add exceptions for fraud and unauthorized-transaction prevention, legitimate and documented risk management, and lawful state or foreign restrictions on offering a service.
CLEAR § 7(a)–(b) (particularized orders, notice)	GENIUS Act issuer capability to comply with lawful orders; BSA/OFAC blocking; non-disclosure orders	Low to Moderate	Requiring that orders name the person or account, and giving notice as promptly as the order lawfully permits, is compatible with most federal process. Confirm it does not impede orders that carry non-disclosure requirements.
CLEAR § 7(c) (standing-rule ban) and § 8 (federal-compliance exception)	BSA/AML program and transaction-monitoring requirements; OFAC screening; GENIUS Act; bank safety-and-soundness and fraud-control practices	High	§ 8 excuses only an action "specifically required" by an identified federal statute, regulation, or order. General AML-program and sanctions-compliance duties, fraud controls, and risk-based holds are mandated in general terms, so § 7(c) may bar practices federal supervisors expect. Impossibility is addressed only in § 24(e). Broaden § 8 to "required, or taken in good-faith compliance with, federal law or supervisory requirements having the force of law," retain the least-restrictive and notice conditions, and add a fraud exception.
CLEAR § 23 and § 24(b) (anti-debanking; enforceable against national banks)	National Bank Act (12 U.S.C. §§ 24, 25b); 12 C.F.R. part 7; FCUA; <i>Cantero</i>	High	§ 23 covers account and payment services of depository institutions generally, and § 24(b) asserts enforceability against national banks. A national bank or federal credit union will argue that the rule prevents or significantly interferes with its powers. § 17(c) disclaims regulation of chartered powers, which helps only for the assurance provisions. Limit § 23 to tokenized deposits and ramp services if retained.
CLEAR § 10 (warrant standard for Wisconsin governmental entities); § 10(c) data-purchase ban	Supremacy Clause; intergovernmental immunity; federal-state data-sharing and child-support, tax, and benefits-verification mandates	Low	§ 10(a) expressly applies only to Wisconsin governmental entities and "does not purport to limit process issued by or to an authority of the United States," which avoids intergovernmental-immunity problems. Confirm that federally required state data matches and civil and regulatory functions (tax, child support, unemployment, Medicaid asset verification) are not unintentionally blocked by excluding administrative subpoenas.

Bill / provision	Federal law implicated	Risk	Why, and how to reduce it
CLEAR § 11 (privacy declaration) and § 25(f) (suppression)	U.S. Const. amend. IV (as interpreted by federal courts); Wisconsin separation-of-powers doctrine	Moderate (state-law risk)	A legislature cannot fix the meaning of art. I, § 11 or of the Fourth Amendment; courts may disregard the "for purposes of the constitution" language while still applying the statutory rule. A statutory exclusionary remedy raises Wisconsin separation-of-powers questions. Recast as a statutory rule that ledger data is not "publicly available information" and as a statutory expectation-of-privacy rule for state statutes, and have LRB review § 25(f).
CLEAR § 12 (private data duties)	GLBA (15 U.S.C. § 6807 preserves more protective state law); BSA reporting; FCRA	Low to Moderate	State privacy laws more protective than GLBA are generally preserved. Conflicts arise where a duty bars disclosure that federal law requires; § 12(a)(2) excepts disclosures "required by law." Check treatment of data-vendor and processor flows.
CLEAR § 13 (privacy-enhancing technology)	18 U.S.C. § 1960; FinCEN guidance on convertible virtual currency mixing; OFAC; <i>Van Loon v. Department of the Treasury</i> (5th Cir. 2024); SAR guidance	High for § 13(a); Low for a state-agency-only § 13(b)	§ 13(a) imposes a duty to offer privacy options, defined to include mixing, with a private right of action, while preserving statutory and regulatory duties. Guidance, exam manuals, and supervisory expectations are expressly overridden, which sets up a direct conflict with how federal supervisors treat mixers. A state-agency version of § 13(b) (no state agency may treat lawful use of privacy tools as suspicious or a basis for denial) is low risk.
CLEAR §§ 14–16, 18 (transparency)	First Amendment compelled disclosure (<i>Zauderer v. Office of Disciplinary Counsel</i> , 471 U.S. 626 (1985)); GENIUS issuer disclosure rules; BSA SAR confidentiality; OCC and NCUA preemption	Low to Moderate	Factual, non-controversial disclosure of controls is a classic consumer-protection tool. § 16(b) already excludes information federal law prohibits disclosing, and § 16(d) keeps screening logic confidential. Preemption risk arises where federal law prescribes issuer disclosures. Personal-identity disclosure of key holders (§ 15(a)(1)) is more a safety and fintech-pushback issue than a federal one.
CLEAR § 17 (assurance of controls)	OCC/NCUA examination authority; visitorial powers (12 U.S.C. § 484)	Moderate	§ 17(b)–(c) are drafted carefully (certification and existing audit materials only; no examination-like access). The non-bank pre-deployment examination (§ 17(a)) is mainly an industry-burden and dormant-commerce issue.
CLEAR §§ 19–20, 22 (self-custody, validation, state restraint)	10th Amendment anti-commandeering (<i>Printz</i> ; <i>Murphy v. NCAA</i>); federal money-transmitter law (18 U.S.C. § 1960; FinCEN MSB rules); Wisconsin ch. 217 (verify)	Very Low for § 22; Low to Moderate for §§ 19–20	State agencies deciding how they pay and are paid, and whether to join a CBDC, exercise core sovereign authority. §§ 19–20 bar only state licensing and penalties; they cannot immunize anyone from federal law and should say so.
CLEAR § 21 (non-programmable payment guarantee for merchants and billers)	Federal payment-network rules; E-SIGN; utility regulation	Low to Moderate	Private mandate, but conditional on the merchant "requiring" programmable money, with a revenue threshold and agency exemptions. State public-utility regulation of essential-service billers should be coordinated.
CLEAR §§ 25, 27, 29 (liability, nexus, jurisdiction)	Dormant Commerce Clause (<i>National Pork Producers Council v. Ross</i> , 598 U.S. 356 (2023)); due-process limits on personal jurisdiction; Federal Arbitration Act	Moderate	Strict liability with statutory damages and deemed purposeful availment against out-of-state issuers will be tested. The § 27 nexus (residents; state agencies) helps. Private actions may be compelled to arbitration even though the Attorney General's authority is preserved (§ 25(a)).

Bill / provision	Federal law implicated	Risk	Why, and how to reduce it
CAGE Act	31 U.S.C. § 5103; U.S. Const. art. I, § 10; federal grant and program rules; BSA cash reporting (CTR; Form 8300)	Low	The state regulates its own acceptance of federal tender and does not set a private tender rule. Replace "subject to applicable federal law" with enumerated exceptions.

7.2 Expected pushback by sector

Sector	UCC (LRB-0372/P1)	CLEAR (by provision)	CAGE
Fintech and digital-asset firms	Support / Low. Article 12 is the national standard for secured lending and custody structures.	Mixed / Moderate to High. Likely to support §§ 13(b), 18, 19, 20, and the immutable-deployment carve-out. Likely to oppose strict liability and statutory damages (§§ 14(c), 25(i)), public identification of natural-person key holders (§ 15(a)(1)), oracle-provider disclosure (§ 16), pre-deployment independent examinations (§ 17(a)), and the breadth of "covered digital asset" and "controlling person." Will argue 50-state fragmentation and GENIUS preemption. Mitigate with safe harbors, size and activity thresholds, entity-level (not personal) key-holder disclosure, and the § 29 staged effective dates.	Low. Payment processors under government contracts will need cash-handling terms.
National defense, law enforcement, and sanctions community	Neutral / Low.	High for §§ 13(a), 16(b), and the § 7(c)/§ 8 combination; Moderate for § 10(c)–(d). Objections that privacy-tool duties, screening-logic filings with a state official, and limits on standing screening rules impede sanctions, counter-terrorist-finance, and ransomware response; Wisconsin DOJ, sheriffs, and district attorneys will object to the data-purchase ban and the bulk and reverse search limits. § 10(a) is helpful because it leaves federal process untouched. Mitigate with an exigent-circumstances provision, a broader federal-law exception, and treating § 10(d) as optional (the draft already labels it so).	Low. Possible concern that cash facilitates laundering; answer with existing BSA cash-reporting duties and the narrow public-payment scope.
Banking industry	Support / Low. Secured-lending clarity, electronic-check processing, and security-procedure clarifications are favorable.	High. Principal targets: § 7(c), § 23 (all accounts and payment services), § 24(b) (national banks), § 12 (data duties, not exempting GLBA-covered entities), § 17(b) (officer certification to the Attorney General), strict liability, and punitive damages. Expect National Bank Act preemption arguments and a fraud-control objection. Mitigate by limiting Part II to tokenized deposits and ramp services, adding fraud and risk-management exceptions, and conforming remedies to existing consumer-protection law.	Low to Moderate. Generally neutral; banks may benefit from government cash deposits.
Credit unions	Support / Low. Benefits from certainty on secured transactions and electronic items.	Moderate to High. Compliance burden for small institutions and reliance on core-processing vendors; FCUA/NCUA preemption. Mitigate with thresholds, vendor flow-down provisions, exclusion of ordinary share accounts without programmable controls, and the § 29(b) staged compliance dates.	Low. Neutral to mildly favorable.

Sector	UCC (LRB-0372/P1)	CLEAR (by provision)	CAGE
Local governments and universities (not among the four sectors named, but decisive for CAGE and CLEAR § 22)	None.	Low to Moderate. § 22 binds political subdivisions and contractors; concern over vendor and ledger choices and litigation exposure under § 25(c).	Moderate. Cash handling, security, and unfunded-mandate concerns under Wisconsin's levy-limit environment. Mitigate with a phased effective date and the "reasonable procedures" language already in § 7.

8. Recommendation

8.1 Scoring against the five criteria

Scores run from 1 to 5, where 5 is best. For "Federal contestability" a 5 means the lowest risk of challenge; for "Industry pushback" a 5 means the least expected pushback among the four sectors you named. Scores are professional judgment, not measurements. The unweighted total is shown for convenience only; the criteria you listed are in priority order, so read Effectiveness first. Because CLEAR is long and its sections differ widely in risk, it is scored by provision cluster.

Bill / provision cluster	Upholding sovereign and constitutional rights	Extensibility	Viability in 2027	Federal contestability (5 = low risk)	Industry pushback (5 = low)	Total (of 25)
LRB-0372/P1 (UCC)	2	5	4	5	5	21
CAGE Act	3	3	4	5	4	19
CLEAR §§ 22, 19–20 (state restraint, CBDC, disbursements, self-custody, validation)	4	4	4	5	4	21
CLEAR § 10 and § 10(c) (government access; data-purchase ban)	5	4	3	4	3	19
CLEAR §§ 14–16, 18 (transparency)	3	5	3	4	2	17
CLEAR §§ 5–6, 7(a)–(b) (nondiscrimination core; particularized orders)	4	4	3	3	2	16
CLEAR § 12 (private data duties)	3	4	3	4	3	17
CLEAR § 21 (merchant and biller non-programmable option)	3	3	3	4	3	16
CLEAR § 7(c) and § 23 (standing-rule ban; all-accounts anti-debanking)	4	3	2	2	1	12

Bill / provision cluster	Upholding sovereign and constitutional rights	Extensibility	Viability in 2027	Federal contestability (5 = low risk)	Industry pushback (5 = low)	Total (of 25)
CLEAR § 13(a) (duty to offer privacy options)	4	3	2	2	1	12
CLEAR § 17 (pre-deployment audits; certification)	2	3	2	3	2	12
CLEAR § 25 enforcement as drafted (strict liability; punitive damages)	4	4	2	3	1	14

8.2 Reasoning by criterion

Effectiveness at upholding sovereign and constitutional rights. CLEAR is the only vehicle that directly addresses automated control, surveillance, and due process. Its strongest rights provisions are the warrant and data-purchase rules (§ 10), the nondiscrimination core (§ 5), particularized orders and reasons (§§ 6–7), and state self-restraint (§ 22), which converts diffuse interests into enforceable rules. CAGE is narrower but self-executing and technology-stable. The UCC is rights-neutral and should be adopted for its commercial benefits.

Extensibility. The UCC is designed to cover similar assets developed in the future on other technologies and is maintained nationally. CLEAR's capability-based definitions (§§ 3(1)–(3), (12)) are the best feature of the draft: they reach new token standards, key-management schemes, and oracle architectures without naming them. CAGE is stable but static, which suits a floor.

Viability in 2027. The UCC and CAGE have the best prospects: the UCC is a nonpartisan uniform act with broad support, though a 106-page bill will need committee time in a budget year; CAGE is short with cross-partisan appeal. CLEAR's state-restraint and self-custody provisions can attract support from privacy-oriented and libertarian-leaning members and from members concerned about access and equity. Its private-sector control rules, strict-liability remedies, and the fact that it is privately sponsored model legislation will slow it if offered as a single bill. The Act's severability and independent-operation provisions (§ 28) make staging practical.

Federal-law risk of contestability. UCC and CAGE are low. CLEAR's state-agency provisions (§§ 10, 19–22) are low. CLEAR §§ 7(c), 8, 13(a), 23, and 24(b) are the most exposed because they intersect with BSA/AML, OFAC, GENIUS Act issuer obligations, and bank and credit-union preemption, and because § 8 is narrower than the introduction implies.

Pushback from fintech, national defense, banking, and credit unions. The UCC draws support from all four. CAGE draws little pushback from these four. CLEAR draws mixed fintech reaction, strong banking and credit-union reaction to §§ 7(c), 12, 17, 23, and 25, and national-security reaction to §§ 13(a) and 16(b). The strategy is to lead with provisions that restrain the state and disclose controls, and to revise or defer provisions that regulate private institutions' operational decisions.

8.3 What I recommend passing, in whole or in part

Bill	Recommendation	Conditions / required amendments
CAGE Act	Pass in whole, with technical amendments.	1) Enforcement: incorporate CLEAR § 25(c) (declaratory, injunctive, or mandamus relief) and an Attorney General role. 2) Define "cash" by cross-reference to "tangible money" (§ 409.102(1)(th) as created) and state that electronic money, stablecoins, deposits, and tokenized cash-equivalents are not cash. 3) Replace "subject to applicable federal law" with enumerated exceptions. 4) Unattended-collection rule: a reasonable cash alternative within a stated distance or time. 5) Disbursements: rely on CLEAR § 22(b) or add a parallel provision. 6) Data minimization for cash-payment records. 7) Use one defined term for government entities across CAGE and CLEAR. 8) Effective date 6 to 12 months after publication; § 5 applies to new, renewed, or amended contracts. 9) Fiscal-estimate and technical-assistance language for local governments.
LRB-0372/P1 (UCC)	Pass in whole, with two targeted Wisconsin amendments.	1) A CLEAR cross-reference and savings clause in ch. 412 (for example in § 412.103): ch. 412 does not limit, and is subject to, Wisconsin law protecting individuals' rights concerning asset controls, privacy, due process, and nondiscrimination, regardless of a CER's jurisdiction under § 412.107. 2) Term alignment: have CLEAR use "qualifying purchaser" (§ 412.102(1)(b)) in § 14(c)(3) and extend the transferee protection to all § 25 remedies. No change to "electronic money" is needed because CLEAR § 22(a)(3) handles CBDC. Keep other text uniform to preserve the national standard.
CLEAR Act	Pass in part in 2027, by section; revise or defer the rest.	See the section-by-section table in Section 8.5. In summary: 2027: §§ 1–4 (as amended), 5–6 (core), 7(a)–(b), 8 (broadened), 9, 10 (with civil-function carve-outs), 11 (recast), 12 (as amended), 14–16 and 18 (tailored), 19–20, 22, 24, 25 (conformed), 26–29. Revise before or defer to 2028: § 7(c), § 13(a), § 17(a), § 21, § 23, § 24(b), § 25(b),(h),(i). Re-verify against current federal rules after GENIUS finalization.

8.4 The CBDC question

CLEAR § 22(a)(3) bars any state agency from adopting, requiring, accepting, or participating in a CBDC arrangement absent express legislative authorization, and § 3(16) defines CBDC broadly. That is Option A from the first report: keep the UCC's "electronic money" definition uniform and address CBDC as state policy. Excluding CBDC from "money" in the UCC (Option B) would give a stronger signal but would leave Wisconsin commercial law unable to treat a lawfully issued federal CBDC as money, creating uncertainty for perfection, take-free, and payment finality and likely drawing banking and fintech objections. If CLEAR § 22 does not pass, an equivalent stand-alone state-restraint provision should accompany the UCC.

8.5 CLEAR section-by-section disposition

Section(s)	Subject	Disposition	Reason / amendment
1–4	Title, findings, definitions, application	2027, amend	Capability-based definitions are a strength. Clarify "technical control" vs. ch. 412 "control"; address validators and AI agents (§ 3(3)); align "state agency" with CAGE; resolve the overlap between "governmental entity" and "state agency"; replace the § 3(3) AI deferral with the AI-agent definition and accountable-person rules in Section 9.

Section(s)	Subject	Disposition	Reason / amendment
5	Prohibited discrimination	2027, narrow	Keep the protected-class, political, religious, lawful-opinion, medical, and social-credit factors. Reconsider "any lawful activity," location, and trade as stand-alone factors; add exceptions for fraud, documented risk management, and lawful state and foreign restrictions.
6	Statement of reasons	2027	Low cost; supports due process. Retain notice-and-cure in § 25(d).
7(a)–(b)	Particularized orders; notice	2027	Compatible with most legal process; confirm interaction with non-disclosure orders.
7(c)	Ban on standing automated rules	Revise or defer to 2028	Overbroad as written (fraud controls, liquidations, escrow, vesting, holder-elected limits). Add holder-elected, disclosed-term, and fraud exceptions, or narrow to rules based on protected factors.
8	Federal-compliance exception	2027, broaden	"Specifically required" is narrower than the introduction's "federal compliance and fraud-prevention exceptions." Broaden to good-faith compliance with federal requirements having the force of law and add a fraud exception, keeping the least-restrictive, notice, and burden conditions.
9	Securities carve-out	2027	Appropriate.
10(a)–(b)	Warrant standard; notice	2027, amend	Add carve-outs for federally mandated data matches and civil functions that rely on administrative subpoenas (tax, child support, unemployment, benefits); add exigent circumstances; assign the Wisconsin procedural citation (ch. 968).
10(c)	Data-purchase ban	2027	Strong, low federal risk; expect law-enforcement objection.
10(d)	Bulk and reverse searches	Optional	Draft already marks it optional; include if sponsors prioritize privacy over investigative tools.
11	Privacy declaration	2027, recast	Replace "for purposes of the constitution" with a statutory rule (not "publicly available information"; statutory expectation of privacy). Courts decide constitutional meaning.
12	Private data duties	2027, amend (or 2028)	Coordinate with GLBA-covered entities; clarify vendor and processor flows. Moderate pushback.
13(a)	Duty to offer privacy options	Defer / delete	Affirmative mandate that overrides federal guidance; high federal and national-security risk. Replace with a state-agency restraint.
13(b)	Safe harbor for privacy tools	2027, limit to state actors	State agencies and state-licensed entities may not treat lawful use of privacy tools, standing alone, as suspicious or a basis for denial; preserve federal law.
14	Disclosure of code and parameters; remedies	2027, amend	Keep binding-disclosure concept and § 14(c)(3) transferee rule (align to "qualifying purchaser"). Review statutory-damages amount and strict-liability exposure.
15	Admin keys and upgrade authority	2027, amend	Disclose roles, mechanisms, thresholds, and addresses; identify entities rather than natural-person signers unless the person is the issuer or operator. Retain security-vulnerability exception.
16	Oracle and compliance-data disclosure	2027	Well-designed tiered structure with a federal-confidentiality carve-out. Confirm the state financial regulator (DFI) has capacity.
17	Assurance of controls	Defer or reduce	Replace pre-deployment independent examination with annual attestation; keep § 17(b)–(c) protections for insured institutions.

Section(s)	Subject	Disposition	Reason / amendment
18	Immutable and ownerless deployments	2027	Sensible, technically informed, consistent with the logic of <i>Van Loon</i> .
19–20	Self-custody, P2P, validation	2027	Confirm interaction with Wisconsin money-transmitter law (ch. 217) and state that federal law is unaffected.
21	Non-programmable payment guarantee	2028 or pilot	State-agency prong overlaps with § 22 and CAGE; merchant and essential-service-biller prongs add private burden. Make CAGE cash acceptance the floor.
22	State self-restraint, CBDC, state payments	2027	Highest-confidence provision; covers disbursements and CBDC.
23	Anti-debanking (all depository account and payment services)	Revise or defer	Overreaches into general banking; limit to tokenized deposits and ramp services, or pursue separately with Wisconsin DFI and federal-alignment analysis.
24	Anti-preemption	2027, amend	Delete or soften § 24(b) (enforceable against national banks); keep § 24(e) impossibility rule. Confirm the claimed federal savings clauses before relying on them.
25	Enforcement	2027, conform	Conform punitive damages to Wisconsin's general cap (Wis. Stat. § 895.043; verify); reconsider strict liability for non-willful violations; replace "Secretary of State" with Wisconsin DFI in § 25(h); route AG and DATCP roles under chs. 100 and 165 (verify); confirm § 25(f) with LRB; § 25(c) is a strong state-restraint remedy.
26–29	Asset-purchase savings, nexus, severability, effective dates	2027	Strong. Use the § 29(b) staged dates, and add compliance periods for banks and credit unions.

8.6 Wisconsin-specific integration checklist for CLEAR

- **Placement and agencies.** The model inserts the Act in the state's unfair and deceptive practices title. In Wisconsin, confirm the right location (for example ch. 100) and the division of authority between DATCP and the Department of Justice. "[State financial regulator]" most likely means the Department of Financial Institutions (DFI), which should also replace "Secretary of State" in § 25(h) (entity registration). Confirm agency capacity and a fiscal estimate.
- **Remedies.** Confirm that the punitive-damages provision does not conflict with Wis. Stat. § 895.043, and that attorney's fees and statutory damages fit Wisconsin practice.
- **Public records and procedure.** Cite the Wisconsin public-records exemption (ch. 19) and the Wisconsin warrant procedure (ch. 968) in §§ 10 and 16(d).
- **State liability.** § 25(c) authorizes suits against state agencies; confirm consistency with Wis. Const. art. IV, § 27 and with notice-of-claim rules (Wis. Stat. § 893.80) for damages claims.
- **Licensing.** § 19 and § 20 interact with Wisconsin money-transmitter and virtual-currency treatment (ch. 217; verify).

8.7 Suggested sequencing

- **Now through Dec. 2026:** secure a bipartisan author pair; have LRB or Legislative Council draft CLEAR into Wisconsin's statutes (Section 8.6); brief the State Bar business law section, bankers, credit-union leagues, county and municipal associations, DOJ, DFI, and DATCP.
- **Jan. to Mar. 2027:** introduce the UCC and CAGE first, then the CLEAR 2027 package as a separate bill so each can move independently; request fiscal estimates early.
- **Throughout 2027:** align effective dates. The UCC takes effect on the first day of the 4th month after publication; CAGE should phase in; the GENIUS Act will be operative (no later than Jan. 18, 2027) as CLEAR moves.
- **2028 session:** revisit §§ 7(c), 13, 17, 21, 23 and the § 25 remedy structure after final GENIUS rules and federal agency positions; consider a title and recording statute for tokenized real estate and a right to withdraw deposits in cash.

9. AI Agents, Legal Personhood, and Accountability under CLEAR

Recommendation. Define an AI agent as a *tool, not a person*. Attach responsibility to named "accountable persons" (natural persons or legal entities that deployed, configured, authorized, or hold administrative authority over the agent). Treat acts by or through an AI agent as the acts of those persons, require disclosure and financial responsibility, and keep CLEAR civil-only. If a criminal provision is retained, limit it to knowing and willful violations by natural persons, with mens rea judged by what the accountable person knew of the agent's configured capabilities. This is a policy recommendation; I am an AI system and have an obvious stake in how the question is framed, so I have grounded the analysis in accountability rather than any view about AI's status.

9.1 Why the question matters for CLEAR

- **CLEAR's only AI provision is a deferral.** Section 3(3) says that if technical control is performed by artificial intelligence or an AI agent, the controlling person "is determined by applicable state law." The Act does not define "AI agent" and Wisconsin has no clear rule for it to defer to.
- **CLEAR's liability model depends on a human or entity.** Civil liability (§ 25(i), strict), damages and compensation (§ 14(c)), attorney's fees and punitive damages (§ 25(b)), Attorney General enforcement (§ 25(a)), and nondiscrimination duties (§ 5) all attach to a "controlling person." If an AI agent holds technical control (§ 3(2)) over a covered digital asset, someone must be identified as the person who answers for it.
- **CLEAR creates no crimes as drafted.** Section 25(g) states that the Act creates no criminal offense. Its drafting option would confine any criminal provision to "a knowing and willful violation by a natural person with intent to deprive another of lawful access." The criminal-liability question therefore arises only if sponsors adopt that option.
- **The risk is a responsibility gap.** Autonomous agents holding keys, session permissions, or administrative roles can freeze, restrict, redirect, or burn assets at machine speed. Without a clear

accountability rule, defendants will argue that no person made the decision, that a vendor is responsible, or that an "ownerless" agent falls outside the Act (§ 18).

9.2 Where Wisconsin law stands today (to be verified with LRB)

Area	Current position	Gap for CLEAR
Statutory "person"	Wis. Stat. § 990.01(26) and the criminal-code definition (ch. 939) cover partnerships, associations, and bodies politic or corporate. Software is not listed.	No statute says whether an AI system is, or can become, a legal person. Courts could be asked to decide.
State AI-personhood exclusion statutes	Idaho (2022), North Dakota (2023), Utah (2024), and Tennessee have enacted statutes denying AI legal personhood. Ohio HB 469 and bills in other states would go further, including barring AI from controlling financial accounts. A separation-of-powers challenge to Utah's law has reportedly been filed.	Wisconsin has no counterpart. These statutes mainly stop courts from recognizing personhood; they do not allocate liability.
Agency law	The Restatement (Third) of Agency treats a computer program as an instrument, not a principal or agent.	The human or entity that uses the program is the principal. CLEAR should say so for covered digital assets.
Electronic agents (UETA / E-SIGN, Wis. Stat. ch. 137; verify section numbers)	Contracts can form through "electronic agents," and actions are attributed to the person on whose behalf the agent acts.	The attribution principle exists for contracts, not for control, freezes, or consumer-protection violations.
UCC (LRB-0372/P1)	Control of a controllable electronic record or electronic money is held by a "person," including through acknowledgment by another person.	An AI agent cannot acknowledge control. Secured-party and holder control must run through a human or entity.
Criminal law	Liability requires a culpable mental state (ch. 939; verify § 939.23 and § 939.24 for intent and recklessness). Party-to-a-crime liability (§ 939.05) reaches persons who aid, abet, or conspire. Entities can be fined; only humans can be imprisoned.	An AI agent cannot form intent or be sentenced. Only the persons who direct, deploy, or knowingly rely on it can face criminal liability.
Damages allocation	Wisconsin applies comparative negligence and limits joint and several liability (Wis. Stat. § 895.045; verify thresholds). Strict product liability may or may not reach software (§ 895.047; verify).	CLEAR's strict liability and the existing allocation rules should be reconciled so that multiple accountable persons share a judgment predictably.

9.3 Options for defining an AI agent in relation to personhood

Option	Effect	Assessment
A. Full legal personhood	The agent can hold assets, sue, and be sued.	Reject. It creates a judgment-proof defendant that could accumulate assets and let humans avoid accountability. Fits none of the five criteria well, and would raise questions about the agent's own rights.
B. Registered entity (DAO-LLC-style wrapper with required human managers, capital, and insurance)	A legal entity, not the AI, is the liable person.	Possible later as an opt-in structure. Still means human managers and an entity; not AI personhood. Not necessary for 2027.

Option	Effect	Assessment
C. Tool with attribution to accountable persons	Acts through the agent are the acts of the persons who deployed, configured, or control it.	Recommended. Mirrors agency law and UETA attribution, is technology-neutral, and closes the "the AI did it" defense.
D. Silence (status quo)	§ 3(3) defers to unspecified "applicable state law."	Reject. Invites inconsistent rulings and the ownerless-agent loophole.
E. Categorical statutory denial of personhood (Idaho / Utah style)	Declares AI is not a legal person for all purposes.	Optional companion bill. Widely adopted and politically attractive, but it only blocks recognition; it does not assign liability, and critics argue categorical declarations can age poorly. Keep any such clause separate from CLEAR so that CLEAR's severability (§ 28) is not burdened.

9.4 Recommended definition and rule architecture

The definition is functional and tied to CLEAR's existing vocabulary, so it does not depend on any model type or vendor. Suggested text for the sponsors (bracketed items require Wisconsin conforming):

Provision	Suggested model text
New § 3(a)(26): AI agent	"AI agent" means a software system, including a machine-learning or other automated decision system, that holds delegated authority over a covered digital asset or over technical control of a covered digital asset and selects or executes actions without contemporaneous human approval of each action.
New § 3(a)(27): Accountable person	"Accountable person" means each natural person or legal entity that (i) deployed, configured, or authorized an AI agent to act with respect to a covered digital asset, or (ii) holds administrative or upgrade authority over the AI agent, or (iii) holds technical control over the covered digital asset through the AI agent.
Replace the last sentence of § 3(a)(3)	If technical control is exercised by or through an AI agent, each accountable person is a controlling person with respect to that exercise.
New § 3A(a): Not a person	An AI agent is not a person, has no legal capacity, and may not be a party to a proceeding or hold property under the law of this state. This section does not affect the formation of contracts through electronic agents under [Wis. Stat. ch. 137].
New § 3A(b): Attribution	An act or omission of an AI agent in the exercise of technical control is the act or omission of each accountable person for purposes of this Act. That an action was taken autonomously, or was not specifically directed or foreseen, is not a defense to civil liability.
New § 3A(c): Agent-held keys and ownerless agents	Cryptographic keys or administrative authority held, generated, or exercised by an AI agent are held by its accountable persons. A person that deploys an AI agent and relinquishes or destroys control over it remains an accountable person for acts of the agent arising from its deployment configuration. Section 18(b) does not relieve that person of duties under this Act.
New § 15(a)(4): Disclosure	A controlling person that uses an AI agent to exercise technical control shall publicly identify the accountable person or persons and the scope of the agent's delegated authority.
New § 3A(d): Financial responsibility	An accountable person that deploys an AI agent with authority to block, freeze, restrict, expire, reverse, or burn covered digital assets of residents shall maintain [insurance, surety, or a segregated reserve] in an amount of at least [\$____] or as set by [DFI], sufficient to satisfy compensation under § 14(c)(2).
New § 3A(e): Holder-delegated agents	A resident who delegates authority over the resident's own covered digital asset to an AI agent is responsible to third parties as principal. The resident is not liable to himself or herself under this Act for the agent's acts, and a controlling person may not discriminate against the resident because the resident uses an AI agent except as permitted by [§ 5(b)] and disclosed terms.

Provision	Suggested model text
New § 3A(f): Developers	A person that only designs, trains, or supplies an AI agent to others is an accountable person only if it also meets clause (i), (ii), or (iii) of the definition, or if it knowingly supplied the agent for use in violation of this Act. Contractual indemnity among accountable persons is not affected.
New § 3A(g): Criminal liability	[If retained in § 25(g) option:] A natural person who knowingly and willfully directs an AI agent to violate [§§ 5, 7, 14] with intent to deprive another of lawful access is guilty of [offense]. In determining the person's mental state, the person is charged with knowledge of the capabilities the person configured or authorized the agent to use. An entity may be fined. No criminal liability attaches to a person solely because the person is the nominal owner of an AI agent, or for conduct of an AI agent the person could not reasonably have foreseen.

9.5 Who is responsible to pay damages

Scenario	Primarily liable	Notes
An issuer or bank's own AI agent freezes tokens for lawful political activity (§ 5)	The issuer or bank, as controlling person	Civil liability is strict (§ 25(i)); remedies under §§ 14(c) and 25(b).
A fintech deploys a vendor's AI agent that misfires	The deployer, to the resident	Deployer seeks contractual indemnity from the vendor. The vendor is directly liable only if it is itself a controlling person (for example a § 3(13) compliance-data provider) or meets § 3A(f).
A holder delegates the holder's own wallet to an AI agent (e.g., session keys) and a third party is harmed	The holder, as principal	CLEAR is not triggered if the holder is the only person with technical control. The developer may face product-liability or negligence claims if the agent was defective.
A deployer launches an agent with self-held or destroyed keys and walks away	The deployer, under § 3A(c)	Closes the "ownerless" loophole. Without it, § 18(b) could leave residents with no one to sue.
A model developer supplies a general-purpose model that a deployer configures	Generally not the developer	Developer exposure arises from negligent design, defect, or knowing facilitation under existing tort and product law, or § 3A(f).
Harm arises from emergent behavior no one intended	Civil liability: the accountable persons. Criminal liability: none absent knowing and willful conduct	Matches ordinary negligence and strict-liability principles for operators of hazardous systems; avoids punishing the unforeseeable.
Multiple accountable persons share a harm	Allocated under Wis. Stat. § 895.045 and any contractual indemnity (verify)	Disclosure under § 15(a)(4) helps plaintiffs identify defendants; financial-responsibility rules ensure payment.

9.6 Who serves a criminal sentence

An AI agent cannot be convicted or sentenced. Criminal liability requires a culpable mental state and a person who can be punished. In practice only natural persons (imprisonment, fines, probation) and legal entities (fines and, in appropriate cases, forfeiture) can answer, and only when they themselves had the required mental state. My recommendation is as follows.

15. **Keep CLEAR civil-only (§ 25(g)).** Civil penalties, strict liability, fee-shifting, and Attorney General enforcement already reach controlling persons and, under the rules above, their accountable persons. Strict-liability crimes are disfavored, and existing Wisconsin criminal statutes (for

example theft, fraud, and computer crimes) already apply to people who direct an AI agent to commit those offenses.

16. **If a criminal provision is retained, follow the draft's own option.** Confine it to knowing and willful violations by natural persons with intent to deprive another of lawful access, as the drafting note suggests, with aggregation limits.
17. **Attribute mens rea correctly.** Charge the person with knowledge of the capabilities the person configured or authorized the agent to use. This stops "I didn't know the AI would do that" as a defense for a person who built or authorized the capability, without punishing someone for truly unforeseeable emergent behavior.
18. **Entities and officers.** Entities face fines. Officers and employees are liable only for their own knowing participation. No one is criminally liable merely as the nominal owner.
19. **Use civil remedies against the system.** Courts should be able to order the accountable person to disable the agent, rotate or revoke its keys, halt its operation, and disgorge proceeds. These are remedies directed at the accountable person, not punishment of the software.

9.7 Interaction with the other bills, constitutional rights, and federal law

- **UCC (LRB-0372/P1).** Add a sentence to ch. 412 (or in the CLEAR cross-reference clause) that control exercised through an AI agent is control by its accountable person, so secured-party and holder control always run through a human or entity.
- **CAGE.** No change is needed. A contractor that uses AI agents to collect public payments remains a contractor bound by § 5.
- **Constitutional rights.** An AI agent holds no constitutional rights, and nothing in this approach grants it any. A human resident's rights under CLEAR § 5 continue to protect the resident when the resident's delegated agent transacts. Controllers may limit automated agent traffic only by disclosed terms and not as a pretext for prohibited discrimination.
- **Privacy.** AI-driven ledger analytics are "ledger-analytics data" when compiled or scored by a vendor (§ 3(9)). The state-agency purchase ban in § 10(c) therefore reaches AI-enriched data products, and private AI agents processing resident data are subject to § 12.
- **Federal contestability.** A narrow rule on accountability for AI agents that control financial assets is much less exposed than comprehensive state AI regulation. Federal executive action in late 2025 directed scrutiny of state AI laws viewed as burdensome, so tie the provision to CLEAR's consumer-protection and financial-asset context and avoid broad AI-system regulation (verify current status). No federal statute grants AI legal personhood; federal courts have required natural-person authorship or inventorship in the copyright and patent contexts.
- **Industry pushback.** Banks and credit unions will accept deployer accountability but resist insurance mandates for small institutions (use thresholds). Fintech firms will object to developer liability and to key-holder disclosure; § 3A(f) limits developer exposure to knowing facilitation or control. National-security stakeholders are largely unaffected because the provision does not limit federal process.

9.8 Scoring and disposition

Provision	Rights	Extensibility	Viability 2027	Federal contestability (5 = low)	Industry pushback (5 = low)	Total (of 25)
AI-agent definition and accountable-person rules (new §§ 3, 3A, 15(a)(4))	4	5	3	4	3	19
Financial-responsibility requirement (§ 3A(d))	3	4	2	4	2	15
Optional criminal provision (§ 3A(g)), as narrowed	3	4	2	4	3	16
Separate categorical personhood-denial statute (Option E)	2	2	4	4	4	16

Disposition. Include the AI-agent definition, attribution, agent-held-keys, and disclosure rules in the 2027 CLEAR package; they are technology-neutral, low in federal risk, and close a gap in § 3(3). Phase the financial-responsibility requirement with thresholds or defer it to 2028 alongside the other deferred provisions. Keep the criminal option out unless sponsors specifically want it. Consider a separate, one-sentence personhood-denial bill only if there is legislative appetite and it is kept out of CLEAR.

9.9 Tracing decision custody when multiple AI agents act with no human in the loop

Core approach. Wisconsin should not try to reconstruct every autonomous decision after the fact. It should (1) require decision custody records created at the time of each action, (2) treat every autonomous action as traceable to a chain of delegated authority, and (3) write rebuttable presumptions that decide who pays when records are missing or unreliable. Under CLEAR's strict-liability model (§ 25(i)), tracing is mainly needed to *allocate* a judgment among defendants, not to establish liability. In criminal cases, tracing is about what a human knew and authorized.

Delegation chain

Every autonomous action traces to authority some person or entity granted: an API credential, signing key, session permission, or administrative role. When Agent A spawns Agent B, which instructs Agent C, each step required a permission someone issued. The **root accountable person**, the human or entity that first authorized the system to act on covered digital assets, remains accountable for downstream acts within the scope of that authority. Each **intermediate accountable person** (a vendor operating an agent or an orchestration layer) is accountable for acts performed under the authority it held.

What a workable decision custody record contains

Layer	What it establishes	Example mechanisms (illustrative, not mandated)
Identity	Which agent acted, in which version	Unique agent identifier tied to a registered accountable person; hashes of model version, system prompt, tool permissions, and configuration
Delegation	Who authorized the agent, and with what limits	Signed, scoped, expiring credentials (capability tokens, smart-account session keys); sub-delegations recorded and revocable

Layer	What it establishes	Example mechanisms (illustrative, not mandated)
Decision record	What the agent saw, decided, and did	Inputs relied on, tool or contract calls made, policy checks passed or failed, human approvals or overrides, and a trace identifier propagated across every agent in the workflow
Integrity and anchoring	That the record was not altered afterward	Append-only, hash-chained logs signed by the agent's key; periodic digests anchored in a ledger or independent transparency log; hardware attestation where available
Revocation and stop controls	When authority ended	Timestamped revocation of credentials; recorded kill-switch events

A single trace identifier passed from agent to agent is the most valuable item, because it lets an investigator assemble a multi-agent sequence from separate logs.

Worked example

Agent A (a compliance screener) flags a resident's tokens on the strength of a third-party data feed; Agent B (an operations agent) freezes them under a credential issued by the bank; Agent C (a treasury agent) redeploys the funds under a credential issued by a fintech partner. The resident's civil claim runs against the bank as controlling person for the freeze (§ 25(i)); against the fintech partner for C's use of the funds if it held technical control; and against the data-feed provider if its output triggered the restriction and it is a controlling person under § 3(13). Allocation among those defendants is then done from the records through contribution and indemnity.

Presumptions and duties to close the gaps

Provision	Suggested model text
New § 3B(a): Decision custody records	An accountable person that deploys an AI agent with authority to block, freeze, restrict, expire, reverse, or burn covered digital assets of residents shall create and retain, for not less than [the limitations period in § 25(j)], records sufficient to identify (i) the AI agent and its configuration at the time of each action; (ii) each person who delegated authority to it and the scope of that authority; (iii) the inputs relied on and the action taken; (iv) any human approval or override; and (v) any revocation of authority. Where an AI agent acts in a workflow with other AI agents, the records shall include an identifier linking each action in the workflow.
New § 3B(b): Integrity	Records under subsection (a) shall be maintained in a form that reasonably detects alteration. The [DFI] may by rule identify acceptable methods, which shall be stated in terms of capabilities and not particular technologies.
New § 3B(c): Presumption on missing or unreliable records	If an accountable person fails to produce records required by this section, or produces records that are not reasonably reliable, the court shall presume that the AI agent acted within the authority granted by that accountable person and may draw adverse inferences against that person. The accountable person may rebut the presumption by clear and convincing evidence.
New § 3B(d): Joint and several liability to the injured resident	Where the records do not permit apportionment of responsibility among accountable persons for the same harm, those accountable persons are jointly and severally liable to the injured resident, with rights of contribution among themselves. This subsection applies in lieu of [Wis. Stat. § 895.045(1)] to the extent of any conflict.
Amend § 6(c): Statement of reasons	The written statement shall also state whether an AI agent made or executed the decision, and identify each accountable person known to the controlling person.
Amend § 15(a)	The public disclosure shall list each AI agent with authority over the covered digital asset, its accountable person, and the scope of the delegation.

Provision	Suggested model text
New § 3B(e): Confidentiality and production	Records under this section shall be produced to the Attorney General or a court under the confidentiality protections of § 16(d). Section 10 does not bar production of records under this section in a civil enforcement action or private action under this Act.
New § 3B(f): Explanation not required	This section requires records of what an AI agent received, did, and under whose authority. It does not require a controlling person to explain or reproduce the internal reasoning of a model.

Criminal cases

- The key evidence is what the human knew when configuring the system, which capabilities they authorized, what warnings they received, and whether they disabled safeguards. Delegation records and configuration history become the core evidence.
- Under the mens rea attribution rule in § 3A(g), a prosecutor traces *forward* from the root authorization rather than reconstructing every downstream decision.
- Where no person knowingly authorized the unlawful capability and the behavior was truly emergent, criminal liability should not attach; civil liability and remedies against the accountable persons cover that case.

Limits to be candid about

- **Records can be falsified, incomplete, or never created.** Signing, anchoring, and independent attestation reduce the risk; the § 3B(c) presumption is the backstop. An adversarial operator can run an agent entirely outside any logging system.
- **Open-source and self-hosted agents** with no identifiable operator remain hard. The deployer rule in § 3A(c) helps, but identifying an anonymous deployer is still an investigative problem.
- **Cross-border chains** raise jurisdiction and evidence-gathering issues. CLEAR § 25(l) reaches those who offer assets to Wisconsin residents but does not solve foreign evidence collection.
- **Privacy tension.** Records contain transaction data, and § 10 restricts state access to resident transaction-graph data; § 3B(e) resolves this for civil enforcement but should be checked with LRB.
- **Admissibility.** Wisconsin's rules on authenticating electronic records and the business-records exception (ch. 909 and § 908.03(6); verify) govern whether these logs are admitted. Counsel should confirm that hash-chained, anchored logs satisfy them.
- **Technology will change.** Define the duty by capability (identity, delegation, decision record, integrity, revocation), not by protocol.
- **Burden and viability.** Record-keeping and presumption provisions will draw pushback from banks, credit unions, and fintech firms on cost, and the joint-and-several rule departs from Wisconsin's general allocation rules. Use thresholds for small institutions, a phased effective date, and treat § 3B as 2027 or 2028 depending on appetite; scored provisionally at Rights 4, Extensibility 4, Viability 2, Federal 4, Industry 2 (total 16 of 25).

10. Items to Verify Before Introduction

20. Whether the bracketed placeholders and any later Solari revisions change the text reviewed here (v1.0-Expanded).
21. The final status of the Anti-CBDC Surveillance State Act and CLARITY Act, and whether GENIUS Act final rules have issued; whether GENIUS preserves state consumer-protection law in the way § 24(a) assumes.
22. Wisconsin statutory references used here (Wis. Stat. §§ 100.20, 165, 893.80, 895.043, 968.373, 968.375; chs. 19, 217, 706, 968) and Wis. Const. art. IV, § 27, with LRB or counsel.
23. The status of *Van Loon* and related sanctions litigation if privacy-technology provisions are pursued.
24. How other states drafted CBDC exclusions, cash-acceptance laws, and CLEAR-type bills, and any litigation that followed.
25. A fiscal estimate for CAGE and CLEAR §§ 22 and 25(c) from DOA and local-government associations.
26. Wisconsin treatment of the personhood and accountability terms in Section 9: Wis. Stat. §§ 990.01(26), 939.22, 939.23, 939.24, 939.05, 895.045, 895.047, and ch. 137; and the current status of the Utah litigation and any federal action on state AI laws.
27. Re-score viability once the November 3, 2026 results fix the legislative and gubernatorial configuration.

Important notice. This report is a policy and legal analysis prepared for legislative planning. It is not legal advice and does not create an attorney-client relationship. Statutory and case citations should be verified by counsel or the Legislative Reference Bureau before reliance. Federal and market developments cited were current as best as could be determined on October 11, 2026 and may have changed.

Appendix A. Principal Authorities Referenced

Category	Authority
Federal constitutional	U.S. Const. art. I, § 8, cl. 5 (coin money); art. I, § 10, cl. 1 (states and tender); amends. I, IV, V, X, XIV
Federal statutes and orders	31 U.S.C. § 5103 (legal tender); Bank Secrecy Act (31 U.S.C. § 5311 et seq.); Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.); E-SIGN (15 U.S.C. § 7001 et seq.); GLBA (15 U.S.C. § 6801 et seq.); National Bank Act (12 U.S.C. §§ 24, 25b, 484); 18 U.S.C. § 1960; GENIUS Act (July 18, 2025); EO 14178 (Jan. 2025); Aug. 2025 executive order on fair banking; Mar. 2025 executive order on payments to and from federal accounts
Federal cases	<i>Carpenter v. United States</i> , 585 U.S. 296 (2018); <i>United States v. Miller</i> , 425 U.S. 435 (1976); <i>NRA v. Vullo</i> , 602 U.S. 175 (2024); <i>Skinner v. Railway Labor Executives' Ass'n</i> , 489 U.S. 602 (1989); <i>Mathews v. Eldridge</i> , 424 U.S. 319 (1976); <i>Fuentes v. Shevin</i> , 407 U.S. 67 (1972); <i>Printz v. United States</i> , 521 U.S. 898 (1997); <i>Murphy v. NCAA</i> , 584 U.S. 453 (2018); <i>Cantero v. Bank of America</i> , 602 U.S. 205 (2024); <i>Zauderer v. Office of Disciplinary Counsel</i> , 471 U.S. 626 (1985); <i>Tyler v. Hennepin County</i> , 598 U.S. 631 (2023); <i>National Pork Producers Council v. Ross</i> , 598 U.S. 356 (2023); <i>Van Loon v. Department of the Treasury</i> (5th Cir. 2024)

Category	Authority
Wisconsin constitution and statutes	Wis. Const. art. I, §§ 1, 3, 4, 8, 11, 13, 18; art. IV, § 27; Wis. Stat. chs. 401–411 (UCC) and proposed ch. 412; chs. 421–427; ch. 706; ch. 217 (verify); §§ 100.20, 893.80, 895.043, 968.373, 968.375 (verify)
State AI-personhood exclusion statutes	Idaho (2022), North Dakota (2023), Utah (2024), Tennessee; Ohio HB 469 (pending); Restatement (Third) of Agency § 1.04 and comments (computer programs as instruments); Wis. Stat. §§ 939.05, 939.22–.24, 990.01(26), 895.045, 895.047 (verify)
Draft bills	LRB-0372/P1 (2027–28 Legislature); Cash Acceptance by Government Entities Act, draft B4F; Solari Model Consumer Ledger and Electronic Asset Rights Act v1.0-Expanded and its Oct. 6, 2026 legislator introduction