Consumer Ledger and Electronic Asset Rights Act

Solari Model Legislation

Version 1.0 - Expanded

ARTICLE 1. The state's code is amended by adding the following part in the appropriate location of the state's consumer-protection (Unfair and Deceptive Acts and Practices) title:

Part I. SHORT TITLE, FINDINGS, AND DEFINITIONS

SECTION 1. SHORT TITLE

This Act may be cited as the "Consumer Ledger and Electronic Asset Rights Act" or "CLEAR Act."

SECTION 2. FINDINGS AND PURPOSE

The [Legislature] finds that residents and others subject to [state] jurisdiction hold and use value across a widening range of programmable digital assets, including, but not limited to, stablecoins, tokenized deposits and securities, and other tokens, each of which can be frozen, restricted, surveilled, or conditioned through code, administrative keys, or external data feeds. This Act protects rights and financial freedom of residents and other persons subject to [state] jurisdiction across all such covered digital assets through four coordinated but independently-operating Parts: nondiscrimination and due process; financial data privacy; code and control transparency; and financial freedom and state operations. Each Part is a distinct exercise of state authority, as set out in the severability provisions.

SECTION 3. DEFINITIONS.

(a) As used in this Act,

(1) "Covered digital asset" means any digital asset or token recorded on a distributed ledger with respect to which any person holds technical control. A covered digital asset need not be a medium of exchange, and includes without limitation payment stablecoins, tokenized deposits, tokenized securities, central bank digital currency, tokenized money-market and Treasury shares, non-fungible tokens, governance tokens, and staked, restaked, or wrapped positions. "Programmable money" is a subset of covered digital assets.

(2) "Technical control" means the ability, whether through code, administrative or upgrade authority, oracle or compliance-data input, ledger permissioning, custodial control, or other means, to create, block, freeze, restrict, condition, expire, reverse, burn, alter, or otherwise affect a covered digital asset or its transfer.

(3) "Controlling person" means any person who holds technical control over a covered digital asset, including, without limitation, a permitted payment stablecoin issuer, depository institution, custodian, exchange, payment processor, smart-contract administrator, permissioned-ledger operator, securities intermediary, and oracle or compliance-data provider.

Affiliate status alone does not make a person a controlling person; it is relevant only to the anti-evasion rule of this Act. If technical control is performed by artificial intelligence or artificial intelligence agent(s), the controlling person is determined by applicable state law.

(4) "Programmable money" means a covered digital asset used as a digital medium of exchange that can be encoded with specific rules or conditions that automatically control its use, including by operation of its governing code or issuer action and including the capability to deny or approve a transaction, impose user-, location-, time-, or party-specific restrictions, expire or diminish its value, or implement a social credit score system.

(5) “Social credit score system” means a system that monitors persons in order to manage, influence, restrict, or control access to financial services using a rating or score based on lawful activities or factors, including the factors described in the nondiscrimination provisions of this Act, and lawful activities concerning firearms, energy, natural-resource or agricultural sectors, lawful advocacy, participation or non-participation in social, environmental, or governance programs, and lawful association with any of the foregoing.

(6) “Resident” means a natural person domiciled in this state or a business or other entity organized under or principally operating under the laws of this state.

(7) “Distributed ledger” means any electronic ledger or database of transactions shared, replicated, or synchronized across one or more nodes, whether public, private, permissioned, or permissionless.

(8) “Transaction-graph data” means distributed-ledger data that identifies, or that when combined with other reasonably available information can identify, the transactions, counterparties, balances, or holdings associated with a resident or other person subject to [state] jurisdiction or such a person’s address or wallet.

(9) “Ledger-analytics data” means transaction-graph data that has been compiled, de-anonymized, aggregated, scored, or enriched by a commercial vendor or other third party.

(10) “Governmental entity” means this state and any of its agencies, departments, political subdivisions, or officers, and any person acting on their behalf. It does not include an agency of the United States or of another state acting under its own authority.

(11) “Privacy-enhancing technology” means any lawful cryptographic or protocol technique—including confidential-transaction, zero-knowledge, mixing, or self-custody technique—that limits the disclosure of the identity or transaction details of a resident or other person subject to [state] jurisdiction.

(12) “Administrative or upgrade authority” means any key, permission, or mechanism by which a person may create, alter, freeze, reverse, mint, burn, pause, or upgrade a covered digital asset or the code governing it.

(13) “Oracle or compliance-data provider” means any person or service that supplies an external data feed, blocklist, allowlist, sanctions or eligibility determination, category or geographic screen, or other similar information, that a programmable system uses to determine whether a transaction is permitted, denied, delayed, restricted, reversed, or reported.

(14) “Insured depository institution” means a bank or credit union whose deposits are federally insured.

(15) “Immutable deployment” means a covered digital asset whose governing code cannot be altered and over which no person holds administrative or upgrade authority. “Ownerless” means no person holds such authority.

(16) “Central bank digital currency” means any digital money issued or directly backed by a central bank or monetary authority, including any digital form of a sovereign currency.

(17) “State agency” means any department, agency, board, commission, or political subdivision of this state, and any officer or contractor acting on its behalf.

(18) “Self-custody” means holding a covered digital asset directly through means that give the holder exclusive control of the cryptographic keys, without reliance on a custodian.

(19) “Validation” means the process of operating a node or otherwise participating in the consensus or transaction-verification process of a distributed ledger network.

(20) “Non-programmable payment option” means cash, a non-electronic payment instrument, or an electronic payment instrument that carries no programmable restriction.

(21) “Essential-service biller” means a provider of electricity, gas, water, telecommunications, or another service considered essential by [agency].

(22) “Fiat on- and off-ramp services” mean services provided for persons to purchase covered digital assets using fiat money and to receive fiat money upon the sale of covered digital assets.

(23) "Machine-readable form" means a structured, openly documented digital representation of information that can be retrieved, parsed, and processed by software without manual re-entry or human interpretation, expressed in a non-proprietary format that is freely available for use without license or fee [or in a format designated by the Attorney General by rule or published guidance]. Information is not in machine-readable form if it is available only as a scanned or rendered image, a flat narrative document, or another format from which the material terms cannot be reliably extracted and evaluated by automated means.

(24) “Material terms” means those features of a covered digital asset’s governing code and parameters that could reasonably affect a resident’s or other person’s ability to hold, use, transfer, or realize the value of the asset, including any capability described in Section 14(a), any administrative or upgrade authority, any fee, expiration, reserve, or collateral parameter, and any oracle or compliance-data dependency.

(25) “Public disclosure,” “publicly disclose,” or “publicly identify” means posting on a publicly accessible website maintained by the controlling person, in plain language and in machine-readable form, unless a section of this Act specifies otherwise.

SECTION 4. APPLICATION

The duties and restrictions of this Act apply to covered digital assets used or held by residents and other persons subject to [state] jurisdiction. The payment-specific duty to offer a non-programmable alternative applies to programmable money. For purposes of the conduct and transparency duties, “controlling person” includes any person holding technical control over the covered digital asset.

PART II – NON-DISCRIMINATION AND DUE PROCESS

SECTION 5. PROHIBITED DISCRIMINATION

(a) It is an unfair and deceptive act or practice, and unlawful, for a controlling person to deny a transaction, allow a transaction to fail, or restrict or terminate service with respect to a covered digital asset used or held by a resident or other person subject to [state] jurisdiction, whether by direct action, omission, automation, algorithm, artificial intelligence, code, or any other means, based in whole or in part on any of the following factors:

(1) Sex, race, skin-color, ethnicity, or sexual orientation;

(2) Political opinion, affiliation, or speech;

(3) Religious beliefs, religious exercise, or religious affiliation;

(4) Any other lawful opinions, affiliations, or speech;

(5) Medical history, including diagnosis, vaccination status, or participation/non-participation in any treatment or procedure;

(6) Purchase and/or browsing history;

(7) Geographical location, place of residence, or location history;

(8) Trade, profession, or business activity, including within a particular industry;

(9) Any lawful activity; or

(10) A rating, scoring, analysis, tabulation, or action related to a social credit score system or similar evaluation.

(b) Nothing in this section prohibits a controlling person from declining a transaction that is itself a criminal offense or payment for a criminal act, subject to the lawful-order due-process and federal-compliance provisions of this Act.

SECTION 6. RIGHT TO A STATEMENT OF REASONS

(a) A controlling person shall provide a phone number, physical address, and electronic mail address for communication to residents or other persons subject to [state] jurisdiction that are holders and users of the covered digital asset.

(b) A resident or other person subject to [state] jurisdiction affected by a denial, failure, restriction, or termination described above may, within ninety (90) days, request a statement of specific reason(s) by phone, mail, or electronic mail from the controlling person making the action.

(c) Within thirty (30) days of the request, the controlling person shall provide a written statement that (i) explains the specific basis for the action, including any speech, religious exercise, business activity, or other conduct that influenced it; (ii) attaches the terms of service relied upon, with citation to the specific term; and (iii) provides a phone number, email, and physical address for further inquiry.

SECTION 7. LAWFUL ORDER DUE PROCESS

(a) Particularized order required. A controlling person shall not block, freeze, restrict, or terminate service with respect to a covered digital asset used or held by a resident or other person subject to [state] jurisdiction pursuant to any lawful order, governmental directive, or regulatory command unless the order specifically identifies, by name, account number, or other particularized designation, the person or account to be affected.

(b) Notice. The affected resident shall receive notice of the restriction and its basis as promptly as the terms of the applicable order lawfully permit.

(c) No standing non-individualized rules. A controlling person shall not implement any standing, automated, algorithmic, or code-based rule that blocks, freezes, expires, restricts, or terminates a resident's covered digital asset based on general categories of conduct, geography, industry, or transaction type absent a particularized order, except as permitted by the federal-compliance exception of this Act. Compliance with a particularized order satisfying this section is not a violation of this Act.

SECTION 8. FEDERAL-COMPLIANCE EXCEPTION

A controlling person does not violate this Act by taking an action that is (a) specifically required by an identified and valid federal statute, regulation, or order; (b) implemented in the least restrictive manner consistent with that requirement; and (c) accompanied by the maximum notice, explanation, and error-correction the applicable federal law permits, including prompt release upon a false-positive determination, a defined release timeline, and correction of erroneous records. The controlling person bears the burden of establishing each element.

SECTION 9. SECURITIES-LAW TRANSFER RESTRICTIONS AND GOVERNANCE EXCLUDED

The nondiscrimination prohibitions of this Act do not apply to any transfer restriction required or contemplated by a valid federal or state securities law or court or regulatory order, or the terms of the instrument as disclosed to holders at issuance, including restrictions under relevant federal regulations, contractual lockups, and transfer-agent controls. The governance and voting mechanics of any entity, protocol, or tokenized instrument are not subject to this Act. This section does not exempt discriminatory or non-individualized blocking that is not required by securities law.

PART III – FINANCIAL DATA PRIVACY

SECTION 10. GOVERNMENTAL ACCESS TO LEDGER DATA

(a) Warrant standard. A governmental entity, or any person acting on behalf of or under contract with a governmental entity, shall not access transaction-graph data of a resident or other person subject to [state] jurisdiction except pursuant to a warrant issued upon a showing of probable cause consistent with [state] Rule of Criminal Procedure [ ]. Process other than a warrant meeting the foregoing standard, including an administrative or investigative subpoena or a national-security letter, does not constitute sufficient process under this section. This section governs only the conduct of governmental entities of this state as defined in Section 3 and does not purport to limit process issued by or to an authority of the United States acting under federal law.

(b) Notice to affected person. The custodian of transaction-graph data shall provide notice to the affected person within ninety (90) days of any disclosure made pursuant to this section, unless a court of competent jurisdiction, upon a showing by the governmental entity of a specific and articulable need for continued nondisclosure, orders a delay of notice for a renewable period not to exceed ninety (90) days. Nothing in this section limits the compulsory legal process of a federal court exercising jurisdiction under federal law; provided that voluntary disclosure by a custodian absent legally sufficient compulsory process remains subject to this section.

(c) Purchase loophole closed. A governmental entity shall not purchase, license, receive, or otherwise obtain ledger-analytics data concerning a resident or other person subject to [state] jurisdiction. Data that could not be compelled directly under subsection (a) may not be acquired indirectly by purchase, license, or other commercial arrangement, regardless of whether the seller or licensor is itself subject to the jurisdiction of this state.

(d) No bulk or reverse searches. A governmental entity shall not conduct, or procure from any person, a bulk or reverse ledger search, i.e., a query designed to identify all persons transacting with a given address, protocol, or category, except pursuant to a warrant issued upon probable cause that a specifically described address, protocol, or category has been used to facilitate a specific criminal offense, and that particularly describes the time period, transaction parameters, and scope of the search, narrowly tailored to minimize the inclusion of persons not reasonably suspected of involvement in that offense. *[Drafting note: Subsection (d) is an optional, higher-protection provision; sponsors for whom bulk or reverse-search authority is a higher law-enforcement priority may omit it without affecting the operation of subsections (a) and (b).]*

SECTION 11. STATE PRIVACY DECLARATION

(a) Distributed-ledger data relating to the covered-digital-asset activity of a resident or other person subject to [state] jurisdiction is not “publicly available information” under the law of this state, notwithstanding that it is technically accessible on a public or semi-public network.

(b) For purposes of the constitution, evidence law, and suppression doctrine of this state, a resident or other person subject to [state] jurisdiction retains a reasonable expectation of privacy in transaction-graph data, and does not waive any constitutional, statutory, or common-law privacy right by using a covered digital asset.

(c) Nothing in this section limits or conflicts with the public disclosure duties of Part IV of this Act, which pertain to the governing code, administrative authority, and compliance-data architecture of a covered digital asset generally, and not to the transaction-graph data of any specific resident or other person subject to [state] jurisdiction.

SECTION 12. PRIVATE-SECTOR DATA DUTIES.

(a) A controlling person that processes covered-digital-asset transactions of a resident or other person subject to [state] jurisdiction shall:

(1) collect, retain, and transmit transaction data only as required by applicable law or as strictly necessary to complete and record the authorized transaction;

(2) not sell, license, or otherwise disclose the resident’s or other person’s transaction data to any third party, including any government, except as required by law or with the resident’s or other person’s informed, revocable consent;

(3) delete or de-identify the resident’s or other person’s transaction data when no longer required for the purpose for which it was collected;

(4) notify affected residents and other persons subject to [state] jurisdiction and the Attorney General of any breach of unencrypted transaction data without unreasonable delay; and

(5) not condition the provision of service on the resident’s or other person’s consent to any collection or use of data that is not essential to the service.

SECTION 13. PRIVACY-ENHANCING TECHNOLOGY

(a) Duty to offer. A controlling person shall, where not prohibited by federal or state statute and technically feasible, offer residents and other persons subject to [state] jurisdiction privacy-protective options for their covered-digital-asset activity. For purposes of this subsection, a privacy-protective option is not rendered unlawful by federal or state regulatory guidance, a guidance letter, an examination manual, a supervisory expectation, or a similar non-statutory pronouncement. Nothing in this subsection excuses compliance with an obligation imposed by federal statute or by a regulation having the force of law.

(b) Safe harbor. The lawful use, provision, or development of privacy-enhancing technology is not, standing alone, suspicious activity or a lawful basis for denial or termination of service under the law of this state.

(c) A violation of subsection (a) is enforceable by [the state Attorney General / the state financial regulator] and, additionally, gives rise to a private right of action for [injunctive relief / statutory damages of $___].

PART IV – CODE AND CONTROL TRANSPARENCY

SECTION 14. DISCLOSURE OF CODE AND PARAMETERS

(a) A controlling person that offers a covered digital asset to residents or other persons subject to [state] jurisdiction shall publicly disclose the material terms encoded in the asset's governing code and parameters, including any capability to block, freeze, restrict, condition, expire, reverse, or burn the asset or its transfer.

(b) Code as binding disclosure. The publicly disclosed code and parameters constitute a binding disclosure of the instrument's terms, comparable to a deposit-account agreement. A programmable restriction that has not been disclosed as required by this Act is a violation of this Act and gives rise to the remedies provided in subsection (c).

(c) Remedies.

1. Where the violation arises from the exercise of an undisclosed capability to block, freeze, condition, or restrict, the affected person may obtain an order directing the controlling person to immediately cease application of the undisclosed restriction.

2. Where the violation arises from the exercise of an undisclosed capability to expire, reverse, or burn the asset, or where the effect of the restriction cannot be technically undone, the affected person is entitled to compensation equal to the greater of

(i) the fair market value of the affected asset measured at the time the undisclosed restriction was exercised, or

(ii) actual damages proximately caused by the violation, plus statutory damages of not less than $[_] per violation.

(3) A remedy under paragraph (1) shall not be ordered against a subsequent transferee who acquired the asset for value and without notice of the violation; in such case, compensation under paragraph (2) is the exclusive remedy.

(4) The remedies of this subsection may be sought in a private action under Section 25(b), or by the Attorney General under Section 25(a).

SECTION 15. ADMINISTRATIVE KEYS AND UPGRADE AUTHORITY.

(a) A controlling person shall publicly disclose

(1) the identity of each natural person, legal entity, or set of key-holders possessing administrative or upgrade authority over the covered digital asset

(2) the scope and technical mechanism of that authority (including, where applicable, the relevant contract address, function names, and multi-signature threshold), and

(3) any change in the identity or scope of such authority, within [5] business days of the change.

(b) Upgrade notice. Not fewer than [30] days before a material change, i.e., a change that creates, expands, or eliminates an authority described in subsection (a), or that affects the ability of a resident or other person subject to [state] jurisdiction to transfer, redeem, or access the covered digital asset, the controlling person shall publicly disclose the change and shall notify the [state financial regulator]. Where the controlling person reasonably determines that advance public notice would create a material risk of front-running, manipulation, or exploitation of a security vulnerability, the controlling person may instead (1) make the disclosure contemporaneously with the change's effective time, provided the effective time is delayed not less than [24] hours after that disclosure, and (2) file with the [state financial regulator], no later than the time of disclosure, a written statement of the specific basis for invoking this exception. Invocation of this exception is subject to review by the [state financial regulator], and a pattern of invocation without adequate basis is itself a violation of this Act.

SECTION 16. ORACLE AND COMPLIANCE-DATA DISCLOSURE (TIERED).

(a) Public Tier. A controlling person shall publicly identify by legal name and, where applicable, a description of the specific product or service used, each oracle or compliance-data provider that supplies a screening or eligibility input, the fact that screening occurs, and the general categories of screening applied. The controlling person shall update such disclosure within [5] business days of any change in the identity provider of the categories of screening applied.

(b) Confidential tier. A controlling person shall file the specific criteria, thresholds, and rule logic of such screening with the [Attorney General / state financial regulator] annually and within [30] days of any material change to such criteria. The Attorney General or an independent auditor designated under section (c) may additionally request such information at any time, and the controlling person shall provide it within [10] business days of the request. Nothing in this section requires the disclosure of information whose disclosure is prohibited by federal law, including the confidentiality provisions applicable to suspicious activity reports under the Bank Secrecy Act.

(c) For purposes of this section, "independent auditor" means an auditor approved by the [state financial regulator] and unaffiliated with, and not compensated on a contingent basis by, the controlling person, other than standard audit fees.

(d) Information disclosed under this section is exempt from disclosure under [state Public Records Act citation] and shall be maintained under the same confidentiality protections applicable to [examination reports of state-chartered financial institutions / comparable existing category]. Nothing in this section limits the authority of the Attorney General to bring an enforcement action based on information obtained under this section or to disclose a general finding of a violation, provided the specific criteria, thresholds, and rule logic are not thereby disclosed.

(e) A controlling person that fails to timely comply with this section, or that knowingly provides false or materially incomplete information, is subject to the remedies provided in Section 25.

SECTION 17. ASSURANCE OF CONTROLS; BANKING COORDINATION

(a) Non-bank controlling persons. Before deployment and after any material upgrade, a non-bank controlling person shall obtain an independent examination of the matters publicly disclosed under the transparency provisions of this Act and make the results available to the Attorney General on request.

(b) Insured depository institutions. An insured depository institution shall provide a certification to the Attorney General, executed by a senior officer, of the matters publicly disclosed under the transparency provisions of this Act, together with production of existing audit and examination materials to the Attorney General on request under confidentiality. No provision of this Act authorizes any examination-like access to the systems of an insured depository institution.

(c) Coordination with federal banking law. This Act does not regulate the chartered powers of any national bank or federal savings association, does not authorize any visitorial examination under federal law, and imposes only disclosure duties of general application.

(d) Information provided to the Attorney General under this section is subject to the same confidentiality protections and public-records exemption provided in Section 16(d).

SECTION 18. IMMUTABLE AND OWNERLESS DEPLOYMENTS.

(a) For a covered digital asset with administrative or upgrade authority, the transparency duties attach to the person or persons holding that authority.

(b) For an immutable or ownerless deployment as to which no person can perform a duty, that duty does not apply; a front-end operator that solicits residents or other persons subject to [state] jurisdiction to use such a deployment shall disclose that fact and the known material terms and risks.

PART V – FINANCIAL FREEDOM AND STATE OPERATIONS

SECTION 19. RIGHT TO SELF-CUSTODY AND PEER-TO-PEER TRANSACTION.

A resident or other person subject to [state] jurisdiction has the right to self-custody covered digital assets and to transact peer-to-peer, and the running of software or hardware for self-custody or peer-to-peer transaction is not, by itself, money transmission or an activity requiring a license under the law of this state. No state agency shall penalize a resident or other person subject to [state] jurisdiction for self-custody or peer-to-peer transaction of lawfully held assets.

SECTION 20. RIGHT TO PARTICIPATE IN VALIDATION

A resident or other person subject to [state] jurisdiction has the right to engage in validation, and no state agency shall impose a penalty, license requirement, or money-transmission classification on validation activity by reason of that activity alone.

SECTION 21. NON-PROGRAMMABLE PAYMENT GUARANTEE

(a) A person that requires the use of programmable money for a transaction shall offer a non-programmable payment option free of charge. This duty applies to (i) merchants with annual revenue above [$5,000,000], (ii) any state agency receiving payment from or directing payment to a resident or other person subject to [state] jurisdiction, and (iii) essential-service billers.

(b) An adequate non-programmable payment option includes cash, a non-electronic payment instrument, or a non-programmable electronic option. [Agency] may exempt classes of transactions where a non-programmable option is impracticable, such as remote or unattended transactions, provided an alternative accessible channel is offered.

SECTION 22. STATE OPERATIONS AND SELF-RESTRAINT.

(a) No state agency shall:

(1) impose a programmable restriction on any payment made to or from a resident or other person subject to [state] jurisdiction, or condition a payment on such person's consent to financial surveillance;

(2) condition any benefit, license, permit, or service on consent to financial or personal surveillance or on the use of a particular payment instrument; or

(3) adopt, require, accept, or participate in a central bank digital currency arrangement absent express authorization by the [Legislature].

(b) State payments to residents and other persons subject to [state] jurisdiction shall be available in a non-programmable form at the request of the intended recipient.

SECTION 23. ANTI-DEBANKING COORDINATION (FIAT ON- AND OFF-RAMPS)

(a) A depository institution, money transmitter, or custodian serving residents and other persons subject to [state] jurisdiction shall not deny, terminate, or restrict the account or payment services of such person based on a factor listed in the nondiscrimination provisions of this Act, subject to the federal-compliance exception of this Act.

(b) The due-process and statement-of-reasons protections of this Act apply to account termination and to the denial of fiat on- and off-ramp services, so that the right to enter and exit programmable money is protected alongside its use.

PART VI – COORDINATION, ENFORCEMENT, AND GENERAL PROVISIONS

SECTION 24. COORDINATION WITH FEDERAL LAW; ANTI-PREEMPTION

(a) Parts II and IV of this Act are a consumer-protection law preserved by relevant federal savings clauses; they regulate the abusive exercise of control against residents and others subject to [state] jurisdiction, not the issuance, registration, or qualification of any instrument. Parts III and V rest on the distinct, traditional exercises of state authority identified in Section 28(c), and are likewise entitled to the presumption against federal preemption applicable to matters of traditional state concern.

(b) The nondiscrimination and due-process duties are duties of general application enforceable against national banks and their networks; this Act does not authorize any examination-like access to a bank's systems.

(c) As applied to tokenized securities, this Act reaches only the conduct made unlawful by its nondiscrimination provisions and does not impose any requirement preempted by federal or state law as to a covered security.

(d) Anti-evasion. Affiliate status is relevant only to prevent evasion of this Act through the interposition of a controlled entity; it is not itself a basis of primary liability.

(e) No provision of this Act shall be construed to require conduct that is impossible to perform in simultaneous compliance with a specific mandatory federal obligation; each provision is to be given the broadest effect consistent with federal law, and invalid applications severed.

SECTION 25. ENFORCEMENT

(a) Public enforcement. A violation of this Act is an unfair or deceptive act or practice. The Attorney General may investigate and enforce this Act under [the state UDAP statute] or other relevant legal provision, including by injunction, civil penalty, restitution, and disgorgement. The Attorney General's authority is independent of, and not defeated by, any arbitration agreement or class-action waiver between a controlling person and a resident or other person subject to [state] jurisdiction.

(b) Private right of action. A resident or other person subject to [state] jurisdiction aggrieved by a violation may bring a civil action for declaratory or injunctive relief and actual damages and may recover reasonable attorney's fees. Upon a finding that the defendant acted willfully or repeatedly, the court may in its discretion award punitive damages up to three times actual damages.

(c) State self-restraint. The state-operations and self-restraint duties of this Act are enforceable by any aggrieved resident or other person subject to [state] jurisdiction by an action for declaratory, injunctive, or mandamus relief against the responsible state agency.

(d) Notice and cure. For a first violation of the statement-of-reasons or disclosure duties of this Act that is not knowing or willful and has not caused demonstrable harm to an identifiable resident or other person subject to [state] jurisdiction, punitive damages shall not be awarded, and the Attorney General shall provide written notice of the deficiency and not less than thirty (30) days to cure before pursuing a civil penalty under subsection (a). This subsection does not limit the availability of injunctive relief or a private action for actual damages. *[Drafting option: a narrower version of this subsection would withhold* *only punitive damages for a first, promptly-cured violation, while leaving the Attorney General free to pursue a civil penalty regardless of cure. The broader version above additionally requires notice and a cure opportunity before any civil penalty may be sought, favoring encouragement of prompt voluntary compliance over preserving maximum AG penalty leverage against first-time, good-faith violations.]*

(e) Good-faith safe harbor. A defendant is not liable for damages to an aggrieved resident or other person subject to [state] jurisdiction for action taken in documented good-faith reliance on the federal-compliance exception or a particularized lawful order under this Act.

(f) Suppression. Evidence obtained in violation of Section 10 of this Act is inadmissible in the courts of this state.

(g) No criminal liability. This Act creates no criminal offense. [Drafting option: if a criminal provision is retained, consider confining it to a knowing and willful violation by a natural person with intent to deprive another of lawful access, with aggregation limits.]

(h) Revocation of right to transact business. For repeated and willful violations of this act, the [state] Secretary of State may revoke the right of an entity to conduct business in the state.

(i) Standard of liability. Except where a section of this Act expressly requires a showing of knowledge, intent, or willfulness, a violation of this Act does not require proof of the controlling person's knowledge or intent. This subsection does not alter the heightened probable-cause standard of Section 10 or any section that conditions liability on a particular showing.

(j) Limitations period. An action under this Act must be commenced within three years after the violation occurs, or within one year after the violation is discovered or reasonably should have been discovered by the aggrieved person, whichever is later, but in no event more than six years after the violation occurs.

(k) Non-exclusivity. The remedies provided by this Act are cumulative and are not exclusive of any other remedy available under other law.

(l) Jurisdiction. A controlling person that offers a covered digital asset to a resident or other person subject to [state] jurisdiction is deemed to have purposefully availed itself of the jurisdiction of the courts of this state for purposes of an action under this Act, irrespective of the controlling person's state or country of domicile or organization.

SECTION 26. ASSET SALE OR PURCHASE NOT PROHIBITED.

Nothing in this Act shall be construed to prohibit the lawful purchase or sale of any digital asset by any public or private party.

SECTION 27. NEXUS

This Act applies only to transactions, accounts, and covered digital assets used or held by residents or other persons subject to the jurisdiction of this state, and to the conduct of this state's own agencies.

SECTION 28. SEVERABILITY; INDEPENDENT OPERATION OF EACH PART

(a) The provisions of this Act are severable. Each Part, and each section within a Part, is independently enforceable, and the [Legislature] would have enacted each standing alone.

(b) No mutual dependency. No Part or Section depends on the validity of any other; the invalidity of any provision or its application to any person or circumstance does not affect the validity of the remainder, which shall be given full effect.

(c) Distinct exercises of power. The [Legislature] finds that each Part is a distinct exercise of state authority, i.e., the nondiscrimination and due-process Part and the transparency Part as consumer-protection and unfair-practices law; the privacy Part as an exercise of the state's authority over its own agencies, its own evidentiary and constitutional law, and over private data practices generally; and the financial-freedom and state-operations Part as the state's regulation of itself and as default rules of state law. The [Legislature] intends that a court's characterization of one Part not govern another.

SECTION 29. INTERSTATE CONSISTENCY; EFFECTIVE DATES

(a) This Act shall be construed, to the extent its text permits, consistently with substantially similar Acts adopted by other states, to minimize compliance burdens across jurisdictions.

(b) Staged effective dates. The disclosure and statement-of-reasons duties take effect [six months] before the assurance and transparency-report duties. The remaining provisions of this Act take effect [___].