Received by Legislative Council Staff
3/2/26 at 9:57 am

Construction; enterprise finance in this act; no tax authorization. This act creates and governs the Automation Mitigation Enterprise (the "Enterprise" or "AME") and the Enterprise Mitigation Revenue authorized herein. References in this act to other titles or articles are for coordination and cross-reference only. Any enterprise charge, fee, assessment, penalty, or rate authorized by this act is imposed and administered solely by AME pursuant to this act, is intended to constitute an enterprise charge and not a tax, and no provision of this act shall be construed to authorize a state tax, to create a general-fund appropriation obligation, to require a General Fund backfill, or to confer a general welfare entitlement. The general assembly intends that enterprise charges under this act be reasonably related to the overall cost of providing the enterprise functions, services, oversight, administration, auditing, dispute resolution, and mitigation authorized herein for covered operator activities with a sufficient Colorado nexus, and that such charges be imposed under objective, uniformly administered, and auditable standards adopted by rule. Any enterprise-funded program, mitigation supplement, restricted-purpose disbursement, direct-to-provider payment, or enforcement or mitigation infrastructure expenditure authorized by this act (including secure access pathways, guardianship credentialing, and digital repossession prevention or recovery infrastructure, and non-surveillance compliance infrastructure to prevent, detect, and remediate contraband-output events, including compute-severance controls, output-integrity controls, and audit tooling) is conditioned on certified revenue sufficiency and, if revenues are insufficient, must be implemented by AME on a scaled, pro rata, or phased basis by rule using available, lawfully collected enterprise revenues; provided that no such scale-down, phase rollback, or funding insufficiency shall be construed to reduce, delay, impair, waive, or render unenforceable any prohibition, duty, remedy, penalty, vendor exclusion, debarment referral, clawback, restitution, remediation obligation, or other operator-facing consequence

applicable to contraband-output events or other violations under this act. Any such program must be administered through non-cash design where applicable, including restricted-purpose instruments and direct-to-provider, direct-to-merchant, direct-to-landlord, or direct-to-servicer mechanisms, and shall not be structured as an unrestricted cash benefit to a resident. Any expansion of any enterprise-funded program must be authorized only through an objective phased scale-up pathway tied to objective displacement and/or saturation triggers and certified revenue sufficiency, and must include automatic pro rata scale-down when revenues are insufficient. Any such program must be administered with data minimization, segregation, retention limits, and materially equivalent analog access pathways where applicable, and any use of item-level eligibility identifiers (including UPC, SKU, or PLU) must operate as a one-way eligibility gate only and shall not be used, designed, or reasonably capable of being used to facilitate, conceal, monetize, launder, or finance contraband outputs or contraband-output events, including through prohibited merchant coding, item aliasing, bundling, split-tender structuring, intermediary routing, or other evasion patterns.

Construction; independent operability. This act is intended to be operable independently. Any cross-references to other titles or articles are for coordination only and do not require enactment of any other measure as a condition of effectiveness. No provision of this act shall be construed to imply a unified subject across multiple measures or to alter the single subject stated herein, and no duty, power, remedy, or enforcement authority granted in this act is contingent upon enactment of any companion measure. The provisions of this act shall be construed, to the maximum extent permitted by law, to preserve independent effectiveness of each fee, program, enforcement mechanism, and safeguard that can operate without any invalid, enjoined, or non-enacted provision.

Be it Enacted by the People of the State of Colorado:

Single subject. This act concerns the creation, governance, and administration of the Automation Mitigation Enterprise (AME) as a state enterprise, the authorization and administration of Enterprise Mitigation Revenue as enterprise charges, and self-contained rulemaking, enforcement, dispute-resolution, and remedies provisions to mitigate measurable externalities arising from emergent automation and covered operator conduct within Colorado, including scalable essential-support and mitigation measures implemented through restricted-purpose, non-cash, direct-to-provider or direct-to-servicer disbursements that may be expanded on a phased basis up to full covered-cost payments only upon objective displacement and/or saturation triggers and certified revenue sufficiency, with automatic pro rata scale-down when revenues are insufficient, no general welfare entitlement, and no General Fund backfill, and enterprise-funded compliance and enforcement infrastructure that incentivizes and enforces contraband-data and contraband-output controls, including non-surveillance compliance infrastructure for contraband-output prevention and auditability (such as compute-severance controls and audit tooling). This act shall be construed so that any optional resident-facing mitigation measure is an enterprise-funded, revenue-conditioned service and not an unconditional public benefit; and so that any wallet, voucher, or payment-rail mechanism is administered using minimization, segregation, and retention limits, and any use of item-level eligibility identifiers (including UPC, SKU, SKU-equivalents, or PLU) operates only as a one-way eligibility gate for eligibility and transaction authorization and shall not be construed to permit facilitation, monetization, concealment, or laundering of contraband outputs or contraband-output events. No phase rollback, pro rata scale-down, or suspension of any enterprise-funded mitigation program due to revenue insufficiency shall be construed to reduce, impair, or limit the enforceability of contraband-output

prohibitions, penalties, vendor exclusion, debarment referral, clawback, restitution, remediation, injunctive relief, or other remedies authorized by this act.

SECTION 1. Legislative Declaration.

(1) The general assembly finds and declares that:

(a) Colorado residents and public systems bear measurable externalities and emergency harms arising from emergent automation, automated decision systems, and large-scale commercial data-processing practices, including fraud, identity exploitation, coercion, nonconsensual synthetic depiction, discriminatory consequential decisions, and infrastructure strain;

(b) A dedicated, administrable enterprise is necessary to implement outcome-based mitigation, auditing, and compliance programs, to finance mitigation infrastructure through enterprise charges rather than taxes, and to coordinate restitution, remediation, and deterrence in a manner consistent with article X, section 20 of the state constitution;

(c) Effective mitigation requires enforceable duties, meaningful civil penalties, injunctive relief authority, and auditable compliance standards, together with accessible dispute-resolution processes for residents and regulated entities;

(d) Enterprise charges authorized by this act are imposed for the purpose of funding enterprise services and mitigation programs provided by AME, and are not intended to constitute a tax or a general-fund program.

(2) It is the intent of the general assembly that this Act:

(a) Creates AME as the administering entity and vests AME with the powers and duties necessary to implement this act;

(b) Authorizes AME to adopt rules, administer enterprise programs, conduct audits and investigations, and enforce compliance through administrative orders and civil actions;

(c) Establishes self-contained due process, dispute-resolution, and judicial review procedures

applicable to AME actions under this act; and

(d) Preserves strong enforcement “teeth” through penalties, injunctive relief, restitution and remediation mechanisms, and operator-facing consequences, independently of any companion measure.

(3) EMERGENCY FINDINGS. The general assembly finds and declares that the rapid deployment of artificial intelligence and automated systems constitutes an ongoing emergency affecting the public peace, health, safety, and welfare because (a) a single image, voice sample, or behavioral trace can be used to generate nonconsensual synthetic likeness outputs, including sexually explicit depictions, coerced performances, and impersonations, at population scale and at near-zero marginal cost; (b) such outputs are rapidly replicable and effectively irreversible once distributed, rendering traditional takedown and post hoc remedies inadequate; (c) existing civil and criminal remedies addressing harassment, fraud, or nonconsensual intimate imagery are insufficient to prevent or remedy these harms in real time because they lack standardized, administrable compliance and enforcement mechanisms at the point of commercial deployment and use; (d) unlawful ingestion of resident-protected data and high-speed model replication can compound harms before a resident can obtain relief; and (e) an enforceable, standardized enterprise mechanism to set mitigation standards, verify compliance through audits, and impose swift remedies is necessary for immediate prevention of future harm and for accountable remediation when violations occur.

SECTION 2. In Colorado Revised Statutes, add article 20 to title 24 as follows:
ARTICLE 20

AUTOMATION MITIGATION ENTERPRISE AND ENFORCEMENT

24-20-201. Definitions.
As used in this article 20, unless the context otherwise requires:

"Contraband Data" means any data ingested, processed, stored, trained upon, or used without a valid, cryptographically verifiable authorization token or consent mechanism recognized by rule

by AME, or in violation of an intake-gate, refusal, or always-on veto obligation applicable to a covered operator under Colorado law.

(13) “Item-level eligibility identifier” means an item-level code, token, or identifier, including a UPC, SKU, PLU, merchant item identifier, catalog identifier, or functionally equivalent code, that is used solely to determine whether a specific good or service is eligible for payment, voucher redemption, restricted-purpose credits, or other enterprise-authorized disbursement. An item-level eligibility identifier is a one-way eligibility gate and may be used only for (a) real-time authorization of an eligible purchase; and (b) limited, non-continuous audit, reconciliation, fraud investigation, or dispute-resolution purposes as expressly authorized by rule by AME. An item-level eligibility identifier must be administered subject to minimization, must not be used for continuous monitoring, behavioral profiling, generalized purchase surveillance, resident dossier creation, dynamic pricing, credit scoring, advertising, or any other secondary purpose, and must be segregated from resident identity data where feasible, including through tokenization, hashing, or other technical and administrative separation controls adopted by rule. AME shall adopt by rule clear retention limits for item-level eligibility identifiers and associated logs, consistent with the minimum period necessary to resolve payment disputes, complete required audits, and satisfy record-retention requirements applicable to the enterprise, after which such data must be deleted or irreversibly de-identified. Nothing in this definition authorizes use of UPC, SKU, PLU, or similar identifiers as inputs to infer, reconstruct, or profile resident behavior beyond eligibility determination for the specific transaction, or to generate or support a “safe harbor” or compliance credit based on expanded resident-level tracking, or to expand the scope of payment-rail logs beyond what is necessary to execute and audit the specific restricted-purpose transaction, or to facilitate, conceal, monetize, or launder contraband outputs

or contraband-output events, including through item aliasing, bundling, prohibited merchant coding, split-tender structuring, intermediary routing, or other evasion techniques.

(14) "Covered entity" or "covered operator" means any person or business entity that deploys, operates, offers, sells, licenses, leases, or provides an automated decision system, emergent automation system, or other covered automated processing service in Colorado, or that commercially delivers such a service to or targets Colorado residents, and includes any person that retains operational control through authority, license, or delegation, as further defined by rule by AME.

(15) Delegated system; operator responsibility. Any model, automated system, tool, contractor, processor, or service operating under the authority, license, or delegation of a covered entity is deemed an extension of that covered entity for purposes of duties, enforcement, and liability under this article, regardless of subcontracting or vendor arrangements.

24-20-202. Automation Mitigation Enterprise — creation — powers — duties — rulemaking.

(1) There is hereby created the Automation Mitigation Enterprise (AME), which is a government-owned business operating as a state enterprise.

(2) AME shall:

(a) Administer this article and any enterprise programs established herein to mitigate measurable externalities

arising from covered operator activities;

(b) Receive, process, and investigate complaints alleging violations of covered operator duties enforceable under this article, including contraband-data ingestion and unlawful automation-enabled identity exploitation, as applicable;

(c) Conduct audits, inspections, and compliance reviews of covered operators subject to this article, including review of records, attestations, and technical compliance evidence, subject to confidentiality protections established by rule;

(d) Issue administrative compliance orders, cease-and-desist orders, remediation orders, and penalty assessments as authorized by this article;

(e) Establish and administer accessible dispute-resolution processes for residents and covered operators, including informal resolution pathways and formal adjudicatory hearings for contested agency actions;

(f) Maintain and publish guidance, technical standards, and compliance materials necessary to implement this article, and publish annual transparency reports containing aggregate statistics, enforcement actions, and audit summaries, while protecting resident privacy and trade secrets;

(g) Coordinate with the attorney general and other state agencies regarding civil enforcement actions, collections, and referrals as authorized by this article; and

(h) Adopt and enforce, by rule, minimization, separation, retention, anti-dossier, and analog-access guardrails applicable to any enterprise-administered or enterprise-required verification service, restricted-purpose disbursement mechanism, direct-to-merchant or direct-to-provider payment rail, wallet, voucher, or item-level eligibility identifier workflow, including prohibitions on continuous monitoring and generalized tracking; prohibitions on commingling item-level eligibility identifiers with resident identity data where feasible segregation controls exist; restrictions requiring non-cash design (no cash withdrawals and no cash-equivalent resident payout functionality) for enterprise-funded restricted-purpose benefits; and enforceable retention limits for payment-rail and authorization metadata;

(i) Establish, by rule, essential-support mitigation categories and eligibility standards for restricted-purpose, direct-to-provider disbursements as mitigation measures tied to measurable automation displacement harms and other measurable externalities within the enterprise purpose, including categories such as child care access, essential health and behavioral health supports, housing stability supports limited to primary-residence obligations, workforce transition and training supports, and other essential supports authorized by this article, provided that any such

disbursement authority is conditioned on certified enterprise revenue sufficiency and does not create a general welfare entitlement; and

(j) Fund, as eligible enterprise administration, enforcement, and mitigation-infrastructure costs, secure non-surveillance mechanisms to prevent, mitigate, and remediate unlawful, coercive, or fraudulent “digital repossession” of resident-controlled accounts, credentials, or restricted-purpose disbursement instruments, including technical controls, incident intake, credential recovery, secure escrow or hold mechanisms, and time-limited restoration workflows, provided that any such funding is for enterprise infrastructure and enforcement operations and not an unrestricted resident cash benefit; and

(k) Fund, as eligible enterprise administration costs, guardianship and fiduciary credentialing, verification, and re-verification workflows, including secure analog issuance, renewal, replacement, and dispute pathways and staffed analog access points necessary to ensure that minors, dependents, and residents with disabilities can access enterprise programs through materially equivalent non-digital methods consistent with this article; and

(l) Fund, as eligible enterprise administration, enforcement, and compliance-infrastructure costs, non-surveillance compliance infrastructure intended to prevent, detect, and remediate contraband-output events and other prohibited outputs under this article, including compute-severance control mechanisms, output-integrity controls, tamper-evident logging and audit tooling, and independent technical verification workflows, provided that such infrastructure is designed and administered consistent with this article’s data minimization, segregation, retention limits, and prohibitions on continuous monitoring and generalized surveillance.

(3) AME may promulgate rules necessary to implement this article, including standards for charges, audits, investigations, confidentiality, trade secret handling, penalty calculation, hearing procedures, enforcement workflow, compliance verification, displacement metrics, certified revenue sufficiency methodology, automatic pro rata scale-down procedures, essential-support category definitions, restricted-purpose direct-to-provider disbursement controls consistent with this article, and objective safe harbor and compliance-credit standards that are narrowly tailored, independently auditable, capped by rule, and do not create incentives or permissions for generalized resident tracking, profiling, or other loopholes inconsistent with this article’s minimization and non-surveillance requirements. In adopting rules for any enterprise-funded essential-support, mitigation, grant, voucher, restricted-purpose credit, direct payment assistance, or similar program authorized by this article, AME shall require an Option B-style phased scale-up pathway that: (a) authorizes expansion, subject to objective displacement and/or

saturation triggers and certified revenue sufficiency, up to full covered-cost payments, delivered through direct-to-provider, direct-to-merchant, direct-to-landlord, or direct-to-servicer mechanisms as applicable; (b) maintains non-cash design where applicable; (c) provides for automatic pro rata scale-down or phase rollback when certified revenues are insufficient; (d) does not create any general welfare entitlement and does not require or permit General Fund backfill; and (e) applies data minimization, segregation, retention limits, and materially equivalent analog access pathways, including administration of any UPC, SKU, PLU, or similar item-level eligibility identifiers solely as a one-way eligibility gate. AME shall further adopt rules to ensure that any braided, matched, or transferred funding authorized under this article (including any Medicaid-related stabilization backfill allocation where authorized) supplements and does not supplant baseline appropriations, and to require auditable maintenance-of-effort or anti-supplantation certifications from recipient agencies or entities to the extent permitted by law.

24-20-203. Enforcement; administrative orders; civil actions; penalties; hearings; judicial review.

(1) Enforcement authority. AME may enforce this article by investigation, audit, issuance of subpoenas as authorized by law, administrative orders, and referral to or coordination with the attorney general for civil enforcement.

(2) Administrative orders. Upon a determination, after notice and opportunity to be heard as provided in subsection (6), that a covered operator violated this article or a rule adopted pursuant to this article, AME may issue an order requiring one or more of the following: (a) compliance and cure; (b) cessation of specified conduct; (c) remediation measures; (d) restitution where authorized; (e) production of compliance attestations; (f) payment of civil penalties authorized by this article; (g) clawback of enterprise-provided credits, offsets, benefits, or other enterprise-administered value transfers obtained or retained in connection with, or tainted by, a contraband-output event, to the extent authorized by this article and subject to any applicable audit and dispute procedures; and (h) vendor exclusion or debarment referral consequences where authorized by this article, including exclusion from eligibility for enterprise-funded contracts,

programs, lending participation, offsets, credits, safe harbors, or compliance credits, as applicable.

(3) Civil actions. In addition to any administrative remedy, AME or the attorney general on behalf of AME may bring a civil action in a court of competent jurisdiction to obtain temporary, preliminary, or permanent injunctive relief, specific performance, restitution, civil penalties, costs, and such other relief as the court deems appropriate to enforce this article.

(4) Civil penalties; factors. Civil penalties assessed under this article must be proportionate and may consider the nature, circumstances, extent, and gravity of the violation; degree of culpability; history of prior violations; ability to pay; effect on ability to continue to provide services to Colorado residents; and such other matters as justice may require, as further specified by rule.

(5) Costs and fees. In any action or proceeding to enforce this article, AME may seek recovery of reasonable costs of investigation, audit, expert review, and enforcement. Where authorized by law and ordered by a court, AME may recover reasonable costs.

(6) Notice; hearings; final agency action. For any contested enforcement action under this article, AME shall provide written notice stating the factual basis and legal authority and shall provide an opportunity for an administrative hearing before a neutral decision-maker designated by AME. A final order constitutes final agency action subject to judicial review as provided by law.

(7) Emergency orders. AME may issue an emergency cease-and-desist or preservation order without prior hearing when necessary to prevent imminent harm or ongoing violations, provided that AME affords prompt post-order notice and an expedited opportunity to contest the order as established by rule.

24-20-204. Essential-support mitigation; phased activation; objective triggers; revenue sufficiency; no entitlement.

(1) Essential-support mitigation categories. Subject to certified revenue sufficiency and the phased activation protocol in this section, AME may administer restricted-purpose mitigation measures in the following essential-support categories, solely to mitigate measurable externalities arising from emergent automation and covered operator conduct within Colorado: (a) child care access and continuity supports; (b) housing stability supports limited to primary-residence rent, mortgage, or verified primary-residence utility obligations; (c) essential health, behavioral health, and crisis stabilization supports; (d) workforce transition and training supports necessary for reemployment; and (e) other essential supports designated by rule that are narrowly tailored to measurable automation displacement harms.

(2) Direct-to-provider disbursements; non-cash design. Any mitigation measure under this section delivered through a wallet, payment rail, voucher, or restricted-purpose credit must be implemented as a non-cash, restricted-purpose instrument and must be disbursed only by direct payment to an approved provider, merchant, landlord, mortgage servicer, licensed contractor, or other verified payee, as determined by rule. Subject to the phased activation and expansion triggers in subsection (3) and certified revenue sufficiency under subsection (4), AME may authorize such direct payments in amounts up to full covered-cost payments for the covered eligible good or service, as defined by rule for the applicable essential-support category, provided that no mitigation measure under this section may be withdrawn as cash or implemented as a general-purpose cash-equivalent. Any wallet or payment-rail implementation must minimize, segregate, and limit retention of authorization and transaction metadata consistent with subsection (5), and must not require continuous monitoring or compile resident

purchase histories beyond what is reasonably necessary to authorize a specific restricted-purpose transaction and to conduct limited audit, dispute-resolution, and fraud controls. Item-level eligibility identifiers, including UPC, SKU, and PLU, may be used only as one-way eligibility gates for transaction authorization and limited audit, reconciliation, fraud investigation, or dispute resolution, and may not be used for generalized purchase surveillance or profiling.

(3) Phased activation; objective triggers. AME shall establish by rule an objective phase structure for activation and expansion of essential-support mitigation measures under this section. At minimum:

(a) Phase 1 (targeted essential supports). AME may activate one or more essential-support categories for a defined class of eligible displaced residents upon a finding, based on objective displacement metrics adopted by rule, that automation displacement has exceeded a trigger threshold for a specified measurement period, and may authorize partial or capped direct-to-provider payments consistent with non-cash design.

(b) Phase 2 (expanded essential supports). AME may expand eligibility and/or categories, and may increase payment levels toward covered-cost payments, upon a subsequent finding that displacement metrics have exceeded a higher trigger threshold or have remained above the Phase 1 trigger for a sustained period, subject to certified revenue sufficiency.

(c) Phase 3 (universal essential supports upon automation saturation). AME may expand up to universal access to one or more essential-support categories and may authorize up to full covered-cost payments for eligible goods or services within those categories only upon an automation saturation finding based on objective saturation metrics adopted by rule, published with supporting aggregate evidence, and subject to certified revenue sufficiency. Nothing in this

subsection (3)(c) requires activation of universal supports or full covered-cost payments; it authorizes an expansion pathway conditioned on the findings and funding in this section.

(4) Certified revenue sufficiency; automatic pro rata scale-down; no entitlement. AME shall not obligate or disburse funds under this section unless enterprise revenues are certified sufficient for the applicable award cycle or benefit period under a methodology adopted by rule. If certified revenues are insufficient to fund full implementation for any activated phase, including any authorized covered-cost payment level, AME shall automatically reduce benefit amounts, covered-cost percentages, durations, or scope on a pro rata, scaled, or phased basis by rule. Nothing in this section creates a general welfare entitlement, a vested right to benefits, or any claim for money damages against the state, AME, or any participating provider based on reduction, suspension, or non-activation due to insufficient enterprise revenues, and nothing in this section requires or permits a General Fund backfill. No reduction, suspension, scale-down, or non-activation under this section shall be construed to reduce, impair, waive, or limit the enforceability of any contraband-output prohibition, contraband-data prohibition, or other duty under this article, or any remedy, penalty, clawback, vendor exclusion, debarment referral, injunctive relief, restitution, or remediation authority available for violations.

(5) Privacy, minimization, segregation, and retention limits; analog bridge. AME shall implement any wallet, payment rail, voucher, or restricted-purpose credit program under this section using data minimization, purpose limitation, role-based access controls, and functional separation between eligibility/identity verification and payment processing, with segregation of resident identity data from item-level eligibility identifiers and transaction authorization data where feasible. AME shall adopt by rule retention limits for authorization and transaction metadata and shall require deletion or irreversible de-identification when no longer necessary for

audit, dispute resolution, fraud prevention, program integrity, or record-retention requirements applicable to the enterprise, and shall prohibit secondary use of such metadata for advertising, profiling, generalized surveillance, or resident dossier creation. AME shall ensure materially equivalent analog access pathways consistent with section 24-20-260(4) and shall not condition essential-support access on digital wallet enrollment, device possession, or continuous data sharing.

24-20-260. Construction — opt-in residents; condition-of-access for government.

(1) Resident opt-in; default no. Nothing in this article requires any resident to enroll, register, or activate optional verification services. Where this framework offers enhanced protections through affirmative registration, the default status for residents is non-participation unless the resident expressly opts in.

(2) Condition of access for government actors. Any state, local, or federal officer, agency, contractor, or requesting party seeking access to any protected resident data, enterprise-held audit materials, or enterprise-administered verification systems governed by this article must comply with AME access controls, logging, minimization, retention limits, segregation requirements where feasible, and lawful-process requirements adopted by rule as a condition of access. Such access controls must prohibit continuous monitoring and generalized tracking and must be designed to prevent creation of resident dossiers. Nothing in this subsection expands governmental authority; it governs the manner of access and accountability when access is sought.

(4) Analog bridge preserved. A resident who elects not to use digital tools must be able to access materially equivalent services through free and accessible analog submission methods and staffed public access points administered or required by AME by rule, and such analog access must not be conditioned on digital wallet enrollment, device possession, or continuous data sharing.

(5) Construction; item-level eligibility identifiers; wallet/payment rail privacy; emergency family and kinship tether supports; digital repossession infrastructure; safe harbor limitations. Nothing in this article shall be construed to authorize AME, any participating provider, or any contractor to (a) collect item-level eligibility identifiers or payment-rail logs except as strictly necessary for authorization and limited audit, reconciliation, fraud investigation, or dispute resolution; (b) use item-level eligibility identifiers, merchant category codes, or wallet/payment-rail logs for continuous monitoring, behavioral profiling, generalized purchase surveillance, or resident dossier creation; (c) commingle item-level eligibility identifiers with resident identity data where feasible segregation controls exist; (d) offer, enable, or permit cash withdrawals or general-purpose cash-equivalent access for any restricted-purpose disbursement administered under this article; or (e) design, use, or permit any wallet, voucher, payment-rail, merchant-category, item-level eligibility, or related mechanism under this article to facilitate, conceal, monetize, or launder contraband outputs or contraband-output events, including through item aliasing, bundling, prohibited merchant coding, split-tender structuring, intermediary routing, or other evasion patterns. AME shall, by rule, require data minimization, technical and administrative separation where feasible, and enforceable retention limits for any such identifiers and logs, and shall require deletion or irreversible de-identification when no longer necessary for the limited purposes authorized herein. Consistent with the emergency mitigation purposes of this article and subject to certified revenue sufficiency, AME may fund or support emergency family,

guardian, and kinship "tether" infrastructure and other enforcement and mitigation infrastructure necessary to permit a minor's or dependent's restricted-purpose disbursements to be administered safely without surveillance, including (I) non-smart analog voucher issuance and replacement processes; (II) limited-scope identity and guardianship attestation and credentialing workflows and periodic re-verification standards that are not repurposed for generalized tracking; (III) secure, time-limited dispute and recovery channels for lost credentials; (IV) staffed assistance points; and (V) non-surveillance mechanisms to prevent, mitigate, and remediate unlawful or coercive “digital repossession” of resident-controlled accounts, credentials, or restricted-purpose disbursement instruments, and non-surveillance compliance infrastructure to prevent, detect, and remediate contraband-output events, including compute-severance controls, output-integrity controls, and audit tooling, provided that no such support may be implemented using continuous monitoring, location tracking, cross-merchant purchase profiling, or any resident cash-out feature and all such expenditures are treated as enterprise administration, enforcement, or mitigation-infrastructure costs rather than resident cash benefits. Any safe harbor, compliance credit, or “white-hat” accommodation recognized by rule must be narrowly tailored, independently auditable, and conditioned on prompt notice, scope-limited activity, preservation of audit artifacts, and remediation, and must not operate to excuse intentional evasion, contraband-data ingestion, contraband-output violations, fraud, coercion, or any unrelated or out-of-scope violation of this article, and must not be transferable, sublicensable, or usable to launder prohibited conduct through a contractor, affiliate, or purported security testing engagement.

SECTION 3. Severability.
If any provision of this act or its application is found invalid, such invalidity does not affect other provisions or applications

that can be given effect without the invalid provision or application, and to this end the provisions of this act are declared severable. It is the intent of the people that any invalidity be construed narrowly so as to preserve independent operability of the remaining enterprise charges, governance provisions, enforcement mechanisms, privacy and minimization safeguards, allocation guardrails, and revenue-conditioned mitigation authorities to the maximum extent permitted by law.

SECTION 4. Effective date — applicability.

This act is necessary for the immediate preservation of the public peace, health, or safety, and takes effect upon passage.

(1) Notwithstanding the immediate effective date, AME shall be operational within thirty (30) days after passage.

(2) AME shall publish interim rules establishing enterprise charge administration, audit and investigation procedures, and enforcement workflows within one hundred twenty (120) days after passage, with phased compliance by covered operator class as specified by rule.

(3) AME shall publish procedures for complaint intake, informal dispute resolution, administrative hearings for contested actions, and judicial review guidance within one hundred eighty (180) days after passage.

SECTION 5. Safety clause.

The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

24-20-270. Restitution and remediation; coordination; no standalone entitlement.

(1) Nothing in this article creates a general welfare entitlement or authorizes issuance of universal resident payments absent a specific settlement, court order, or enforcement resolution and compliance with any applicable phased activation and certified revenue sufficiency requirements established under this article. AME may, as authorized by this article, seek and administer restitution, remediation, or mitigation funding through lawful settlement proceeds,

court-ordered restitution, civil penalties, and enterprise charges, and may coordinate with other state agencies where applicable.

Intent; preservation of core purpose. It is the express intent of the People that the core purpose of this Act—the mitigation of measurable externalities arising from Emergent Automation and the protection of resident sovereignty—be preserved to the maximum extent permitted by law. Any judicial finding of invalidity should be interpreted narrowly to preserve the maximum possible functionality of the Automation Mitigation Enterprise and the resident protections and safety standards established by this Act, independently of any companion measure.