THE SENATE
THIRTY-THIRD LEGISLATURE, 2026
STATE OF HAWAII

S.B. NO. 3184

JAN 2 8 2026

# A BILL FOR AN ACT

RELATING TO DIGITAL ASSETS.

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:**

SECTION 1. The legislature finds that the evolution of financial technology has created demand for secure, regulated institutions capable of providing digital asset services, including custody, staking, and fiduciary transactions. The safekeeping of digital assets, through one-to-one reserves, strong cybersecurity practices, and independent audits, is critical to maintaining consumer confidence and financial system integrity.

The legislature further finds that banks and credit unions are well-positioned to offer trusted digital asset services when supported by clear rules, sound oversight, and modernized financial regulatory frameworks. Enabling these institutions to provide digital asset services in either a fiduciary or non-fiduciary capacity allows for responsible innovation while preserving the legal rights and protections of customers.

The legislature further finds that state-chartered financial institutions must be empowered to meet customer needs

in the digital economy while remaining subject to robust oversight and prudential standards.

Accordingly, the purpose of this Act is to establish a regulatory framework to allow for the safekeeping of digital assets while ensuring continued innovation in digital banking.

SECTION 2. Chapter 412, Hawaii Revised Statutes, is amended by adding a new part to article 3 to be appropriately designated and to read as follows:

**"PART . DIGITAL ASSET BANKING**

**§412:3-A Definitions.** As used in this part:

"Commissioner" means the commissioner of financial institutions.

"Customer" means any person or entity for whom an institution provides digital asset services, including a digital asset account holder or a person on whose behalf the institution acts in a fiduciary capacity.

"Digital asset" means virtual currency, cryptocurrencies, natively electronic assets, including stablecoins and non-fungible tokens, and other digital-only assets that confer economic, proprietary, or access rights or powers.

"Digital asset company" means a business entity that is registered to do business in the State and is licensed under the laws of the State as a money transmitter or under any other applicable digital asset licensing regime, and that is authorized to provide digital asset custody services, digital asset transaction services, or both.

"Digital asset custody services" means the safekeeping or custody of digital assets on behalf of customers by an institution, including maintaining control over the digital assets and any associated cryptographic keys.

"Digital asset services" means any services involving digital assets offered by an institution, including digital asset custody services, staking services, and digital asset transaction services.

"Digital asset transaction services" means services that facilitate the execution of digital asset purchase or sale transactions on behalf of a customer.

"Fiduciary capacity" means acting with trust power pursuant to section 412:8-201 to provide digital asset services on behalf of a customer, including discretionary management or administration of digital assets subject to fiduciary duties.

"Institution" means a bank or credit union chartered or licensed under the laws of the State and authorized to conduct digital asset services pursuant to this part.

"Keys" means a pair of cryptographic codes associated with a digital asset wallet, consisting of a public key and a private key; provided that the public key enables the receipt of digital assets and verification of digital signatures, and the Private key enables the control, transfer, or management of digital assets in the wallet.

"Material cybersecurity incident" means a cybersecurity breach or event that materially compromises the security, confidentiality, or integrity of an institution's information systems or the digital assets under the institution's control.

"Non-fiduciary capacity" means providing digital asset custody services solely for safekeeping, without discretionary authority to manage or transfer the assets, and with legal title and control of the assets remaining with the customer.

"Slashing" means a penalty imposed by a blockchain protocol that results in the forfeiture or reduction of staked digital assets or rewards due to a validator misconduct or failure.

"Staking" means committing digital assets to a blockchain network to participate in the network's operations by validating transactions, proposing and attesting to blocks, and securing the network.

"Staking rewards" means any interest, yield, or other compensation earned by a customer through staking digital assets on a blockchain network.

"Subcustodian" means a third party that an institution uses to hold digital assets on the institution's behalf as part of providing custody services to a customer.

"Wallet" means a digital interface or physical device that stores digital assets or private keys, enabling the owner to securely manage, transfer, and maintain independent control over digital assets.

**§412:3-B Banks and credit unions; digital asset custody services.** (a) An institution may directly provide digital asset custody services to its customers.

(b) An institution may provide digital asset custody services in either a fiduciary capacity or a non-fiduciary capacity, subject to the following:

(1) Fiduciary capacity. An institution shall not provide digital asset custody services in a fiduciary capacity unless it is authorized to exercise trust powers pursuant to section 412:8-201. The institution shall exercise its fiduciary capacity in accordance with all applicable fiduciary duties and standards, including those governing trustees, custodians, and agents; and

(2) Non-fiduciary capacity. An institution may provide digital asset custody services in a non-fiduciary capacity; provided that the institution shall act solely as a custodian for the safekeeping of digital assets and shall not exercise discretionary authority over the customer's digital assets. Institutions acting in a non-fiduciary capacity shall act only on the explicit instructions of the customer and shall not independently manage, transfer, or dispose of the digital assets.

(c) An institution shall enter into a written custodial agreement with each customer before undertaking digital asset custody services. The custodial agreement shall clearly specify whether the institution is acting in a fiduciary capacity or

non-fiduciary capacity for the customer and whether the customer's assets are pooled pursuant to subsection (e). The agreement shall include, at a minimum, the following written disclosures, which shall be prominently presented to the customer:

(1) Digital assets held in custody by the institution are not deposits, obligations, or other liabilities of the institution; and

(2) Digital assets in custody are not insured by the Federal Deposit Insurance Corporation, National Credit Union Administration, or any other federal or state deposit insurance or share insurance program.

(d) An institution providing digital asset custody services shall maintain control over the quantity of each type of digital asset in its custody that exceeds the total quantity of that digital asset owed to customers or required to be held on behalf of customers. The institution shall hold not less than a one-to-one full reserve of each digital asset owed or attributable to its customers and the institution's aggregate holdings of each digital asset shall be greater than the total amount of that asset owed by the institution to its customers.

(e) An institution may hold digital assets of multiple customers in a pooled omnibus custody arrangement; provided that the institution maintains accurate records identifying each customer's interest in the digital assets. An institution may segregate a customer's digital assets in a separate account or digital wallet upon the customer's request or as required by the custodial agreement. Pooled custody of assets shall not relieve the institution of requirements, pursuant to subsection (d), to individually account for and fully reserve each type of digital asset for the benefit of customers.

(f) An institution providing digital asset custody services shall undergo an independent audit of its custodial activities and holdings at least once every calendar quarter. The audit shall be conducted by a qualified independent auditor and shall verify that the institution's holdings of each digital asset exceed the amounts of each digital asset owed or attributable to its customers. The institution shall provide the results of each quarterly audit to the commissioner and shall make the results of each quarterly audit available to its customers upon request.

(g) An institution shall notify the commissioner in writing no later than sixty days before initiating digital asset custody services. The institution shall provide any information required by the commissioner to evaluate the institution's plans, policies, and procedures for compliance with this section.

(h) An institution shall not offer digital asset custody services in a fiduciary capacity without first obtaining written approval from the commissioner. In applying for approval from the commissioner, the institution shall demonstrate that it has satisfied all requirements to exercise trust powers and that it has the necessary expertise, policies, and procedures in place to safely conduct fiduciary digital asset custody services. The commissioner may condition or limit the scope of an institution's authority to offer fiduciary digital asset custody services and may impose supervisory conditions that the commissioner deems necessary to ensure the safety and soundness of the institution and the protection of customers' assets.

**§412:3-C Subcustody; digital assets.** (a) An institution may use one or more subcustodians to assist in providing digital asset custody services without obtaining separate consent from

customers; provided that the use of subcustodians shall be disclosed in each customer's custodial agreement. The use of one or more subcustodians shall not relieve the institution of its duties as a custodian or the requirements of this part, and the institution shall remain legally responsible to the customer for the custody of the customer's digital assets.

(b) An institution may place digital assets into subcustody with the following entities:

(1) A bank chartered or licensed under the laws of the State, another state, or the federal government;

(2) A special purpose depository institution chartered or licensed under the laws of the State or another state; and

(3) A digital asset company that holds a current license under the laws of the State as either a virtual currency business or a money transmitter.

(c) An institution placing digital assets in subcustody shall retain legal control and custody of the assets. The subcustodial agreement shall require the institution to remain the custodial record holder of the assets on behalf of its

customers and the digital assets shall remain the property of the institution's customers.

(d) An institution shall obtain a written agreement with each subcustodian engaged by the institution. Each agreement shall describe the rights and responsibilities of the institution and the subcustodian and require compliance with this part. The institution shall make any subcustodial agreement available to the commissioner for review upon the commissioner's request.

(e) For any digital assets held in subcustody, the institution shall require the subcustodian to maintain a one-to-one reserve of each asset type. The amount of each type of digital asset held by the subcustodian shall at all times be equal to the amount of that asset credited to the institution's customers. Different types of digital assets shall not be commingled for reserve purposes, and assets held by a subcustodian on behalf of an institution shall not be commingled with assets held on behalf of a different institution or person.

(f) An institution shall only use a subcustodian that maintains insurance coverage sufficient to protect against the loss of digital assets due to cybersecurity breaches, theft, or

other adverse events. The institution shall ensure that the subcustodian's insurance is valid, in effect, and adequate to cover the value of assets held in subcustody.

(g) If an institution provides digital asset custody services in a fiduciary capacity, any subcustodian of that institution shall be authorized to exercise trust powers pursuant to section 412:8-201. The institution shall provide notice to the commissioner of its use of a subcustodian in a fiduciary capacity, subject to all notice requirements applicable to its fiduciary custody authority.

(h) Digital assets held in subcustody shall be included in the scope of the institution's quarterly audits conducted for the purposes of section 412:3-B(f). All records relating to digital assets held in subcustody shall be subject to examination by the commissioner.

**§412:3-D Digital assets; staking.** (a) An institution may stake digital assets held in custody on behalf of its customers. Staking services may be provided for digital assets held in either a fiduciary or non-fiduciary capacity, subject to the requirements of this section. Unless otherwise instructed by the customer, an institution may include a customer's eligible

custodial digital assets in its staking program by default; provided that the customer has been notified of required disclosures and given an opportunity to opt out of the staking program to pursuant to subsection (h).

(b) Any digital asset that an institution stakes on behalf of a customer shall remain the property of that customer. Staked customer assets, and any staking awards associated with those assets, shall not be recorded as assets or liabilities on the institution's balance sheet. The institution shall ensure that staked assets are safeguarded and not subject to any lien, security interest, or claim of the institution's creditors. No institution shall encumber, hypothecate, or otherwise use a customer's staked assets for any purpose except for facilitating staking on the relevant blockchain or distributed ledger, and shall not expose the assets to risk of loss except to the extent inherent in the normal operation of the staking process.

(c) An institution may use one or more subcustodians or digital asset companies to facilitate the staking of digital assets on behalf of its customers; provided that the institution shall retain legal control over the staked assets and maintain appropriate oversight of the staking process. The use of one or

more subcustodians or digital asset companies for staking shall not relieve the institution of its duties to the customer under this section, and the institution shall remain responsible for ensuring compliance with all requirements of this section. Any subcustodial or third-party arrangement for staking shall be governed by a written agreement that describes the rights and responsibilities of the institution and the subcustodian or digital asset company that shall require compliance with the provisions of this section.

(d) An institution that stakes digital assets on behalf of customers shall maintain reserves of each digital asset in amounts sufficient to facilitate timely customer withdrawals and transfers. The total quantity of each digital asset type held by the institution, including those held by any subcustodian or third-party provider, shall equal or exceed the total quantity of that digital asset owed to customers. The institution shall ensure that an appropriate portion of each digital asset type remains unstaked or otherwise available to meet customer withdrawal requests promptly, subject to any staking lock-up or unbonding periods disclosed to the customer pursuant to this part.

(e) All rewards, yields, or other benefits earned from the staking of a customer's digital assets shall accrue to the benefit of that customer. An institution may deduct a reasonable fee or commission from staking rewards only if that fee has been disclosed in writing to the customer before providing staking services. Except as otherwise agreed in writing by the customer, the institution shall credit all net staking rewards, after the deduction of any disclosed fees, to the customer's account in the same type of digital asset that generated the rewards. Credits for staking rewards shall be made within a reasonable period after the rewards are received or become available to the institution.

(f) An institution shall notify the commissioner of its intention to provide staking services in writing no later than sixty days before initiating the services, which shall include any information that the commissioner requires to evaluate the institution's plans, policies, and procedures for conducting the staking services in a safe and sound manner. An institution shall not offer staking services without obtaining written approval from the commissioner. If the institution will be staking digital assets in a fiduciary capacity, the institution

shall be authorized to exercise trust powers under state law and shall obtain any necessary approval from the commissioner to engage in the fiduciary staking services.

(g) An institution's digital asset staking activities shall be included in the scope of the institution's quarterly audits conducted for the purposes of section 412:3-B(f). The institution shall implement and maintain written internal policies and procedures to effectively identify, monitor, and manage risks associated with staking, including operational, cybersecurity, slashing, and other risks associated with staking services. The institution shall maintain insurance coverage adequate to protect against potential losses arising from staking activities, including those losses attributable to slashing, cybersecurity breaches, theft, or other adverse events, and shall ensure coverage remains valid, in effect, and sufficient to cover the current value of assets staked on behalf of customers. All records relating to the institution's staking services shall be available for independent audit and examination by the commissioner, consistent with the treatment of non-staked custodial asset records.

(h) Before initiating staking services, an institution shall provide the customer with clear and conspicuous written disclosure of terms and conditions of the staking program. The disclosure shall inform the customer, at a minimum, that:

(1) The institution may automatically stake eligible digital assets in the customer's account unless the customer affirmatively opts out of the staking program;

(2) The key risks associated with staking, such as the potential for loss of staked assets or rewards due to slashing or other network events, and cybersecurity and operational risks inherent in the staking process;

(3) Any applicable lock-up, unbonding, or notice period before staked assets can be withdrawn or transferred, and the implications for the customer's access to digital assets;

(4) The customer's rights and obligations related to the staking service, including the right to discontinue participation in staking at any time and the entitlement to receive staking rewards earned on their assets; and

(5) The amount or rate of any fees or commissions that the institution will deduct from staking rewards as compensation for providing the staking service.

(i) A customer's agreement to participate in the staking program shall constitute authorization for the institution to stake the customer's digital assets in accordance with this section. All disclosures required by subsection (h) shall be written in plain language and presented in a manner that is readily accessible and understandable to the customer.

**§412:3-E Cybersecurity; compliance.** (a) An institution shall comply with all applicable federal and state laws and regulations governing its digital asset custody and staking services, including the United States Bank Secrecy Act, P.L. 91-508, Gramm-Leach- Bliley Act, P.L. 106-102, customer due diligence requirements issued by the United States Department of the Treasury's Financial Crimes Enforcement Network, and sanctions administered by the United States Department of the Treasury's Office of Foreign Assets Control.

(b) An institution shall establish and maintain an anti-money laundering compliance program that is risk-based and commensurate with the nature and scope of the institution's

digital asset custody staking services. The program shall include:

(1) A system of internal controls to ensure ongoing compliance with the Bank Secrecy Act, P.L. 91-508, or other applicable anti-money laundering requirements;

(2) An independent testing for compliance to be conducted by qualified internal audit personnel or an independent external party;

(3) The designation of a Bank Secrecy Act and anti-money laundering compliance officer or officers responsible for coordinating and monitoring day-to-day compliance with the program; and

(4) Appropriate risk-based procedures for conducting ongoing customer due diligence, including monitoring customer transactions and updating customer information as necessary.

(c) An institution shall implement and maintain a written cybersecurity program designed to ensure the security of the institution's digital asset custody and staking systems, and to protect the confidentiality, integrity, and availability of customer digital assets and related information; provided that

the cybersecurity program shall be commensurate with the institution's size and complexity and the sensitivity of the institution's operations and shall align with the applicable federal cybersecurity standards for financial institutions, including the Federal Financial Institutions Examination Council Information Technology Examination Handbook and standards established by the National Institute of Standards and Technology; provided further that the program shall comply with applicable federal financial privacy and data security requirements. The cybersecurity program shall include appropriate administrative, technical, and physical safeguards to protect against anticipated threats or hazards and unauthorized access to or theft of customer asset information.

(d) An institution shall notify the commissioner as soon as possible and in no event later than seventy-two hours after discovering any material cybersecurity incident that impacts the institution's digital asset custody or staking systems or the digital assets held or managed through those systems. The institution shall include in the notice a description of the incident and its likely impact on the institution and its

customers. The notice shall be given in accordance with procedures prescribed by the commissioner.

(e) An institution shall maintain detailed records of its compliance efforts under this section, including all policies, procedures, risk assessments, audit reports, and training materials related to its anti-money laundering program and cybersecurity program. All records and supporting documentation shall be retained for a period of at least five years and shall be made available for inspection by the commissioner upon request or during any examination.

(f) Each institution shall designate qualified individuals responsible for overseeing the institution's anti-money laundering compliance program and its cybersecurity program. The designated anti-money laundering compliance officer and the designated cybersecurity program officer shall have the appropriate expertise, authority, and resources to administer their respective programs and to enforce compliance with all applicable laws and regulations. An institution shall promptly report to the commissioner the names and contact information of the persons designated as the anti-money laundering compliance

officer and cybersecurity program officer and shall notify the commissioner of any changes to the designations.

(g) The commissioner may adopt rules and regulations as necessary to implement, clarify, and enforce the requirements of this section, including more specific standards for cybersecurity programs, definition of terms, and detailed requirements for anti-money laundering and customer due diligence programs for digital asset custody and staking services. The commissioner may also issue advisory guidance to assist institutions in complying with the provisions of this section.

**§412:3-F Fiduciary digital asset transaction authority.** (a) An institution shall exercise trust powers under state law only when acting in its fiduciary capacity to facilitate the purchase or sale of digital assets on behalf of a fiduciary account or customer, subject to the requirements of this section.

(b) An institution shall execute a digital asset transaction under this section only:

(1) Pursuant to the express instruction of the customer for whom the institution is acting as a fiduciary; or

(2) In the exercise of discretionary investment authority granted to the institution under the governing fiduciary instrument or applicable law, consistent with the institution's fiduciary duties.

(c) An institution intending to engage in digital asset purchase or sale services under this section shall provide written notice to the commissioner no later than sixty days before initiating digital asset purchase or sale services. The institution shall initiate digital asset purchase or sale services only after the sixty-day notice period has elapsed, unless the commissioner specifies an earlier effective date or objects in writing during the notice period.

(d) Any purchase or sale of digital assets executed under this section shall be affected only through or with a counterparty that is duly licensed or chartered to conduct digital asset business activity.

(e) An institution facilitating digital asset transactions under this section shall act solely in a fiduciary capacity for the benefit of its customers and shall not engage in proprietary trading of digital assets. No purchase or sale of a digital asset shall be made for the institution's own account under the

authority of this section, and all transactions shall be solely for the account or benefit of the fiduciary customer.

(f) An institution facilitating digital asset transactions under this section may use subcustodians or third-party agents to execute transactions on behalf of fiduciary accounts. The institution may delegate discretionary authority to these subcustodians or agents regarding the timing, sequence, and venue of transaction execution. Any delegation shall comply with the fiduciary responsibilities of the institution and be subject to ongoing oversight. The institution shall perform due diligence and maintain continuous monitoring of any subcustodian or execution agent to ensure compliance with this part and the protection of fiduciary assets. Delegation of authority under this subsection shall not relieve the institution of its fiduciary obligations or its ultimate responsibility for compliance with the requirements of this part.

(g) An institution that purchases a digital asset under this section for a fiduciary account shall ensure that the asset is transferred into the institution's fiduciary custody as soon as commercially practicable after the execution of the transaction. All digital assets acquired pursuant to this

section shall be held in custody in accordance with the fiduciary custody standards established in this part, and shall be maintained under the institution's control consistent with its fiduciary obligations.

(h) An institution shall disclose to its customers or persons on whose behalf it acts, before or at the time of any digital asset transaction pursuant to this section:

(1) The methodology or basis used to determine the execution price of the digital asset transaction;

(2) Any spreads, fees, commissions, or other charges that will be applied to the transaction; and

(3) The expected timeline for settlement of the transaction and for the digital asset to be available in the customer's fiduciary account;

provided that any disclosures under this subsection shall be provided in a clear and conspicuous written form and in compliance with any disclosure standards set by the commissioner.

(i) For each digital asset purchase or sale executed under this section, the institution shall create and retain an electronic record of the transaction, including, at a minimum,

the date and time of the execution; the type and amount of digital assets purchased or sold; the price at which the transaction was executed; the identity of the counterparty or any execution agent used; and all fees, commissions, or spreads charged. These records shall be maintained in accordance with applicable record retention requirements for fiduciary accounts and shall be made available to the commissioner upon request or during examination. The institution shall document its compliance with the requirements of this section and shall be prepared to demonstrate compliance to the commissioner.

**§412:3-G Enforcement; supervisory authority.** (a) If the commissioner determines that an institution:

(1) Has violated any provision of this part or any order issued under this part;

(2) Has engaged in any unsafe or unsound practice in connection with its digital asset services; or

(3) Is operating in a manner that threatens the safety or security of customer digital assets,

the commissioner may exercise the enforcement powers pursuant to this section.

(b) The commissioner may issue a written order directing an institution to take specific corrective action to remedy any condition or violation identified under subsection (a). The order shall state the grounds for issuance and the required remedial measures. The institution shall, within ten days of receiving the order, respond in writing to the commissioner detailing the corrective actions taken or that will be taken to address the issues identified by the commissioner. Failure to adequately respond or comply within the ten days may prompt further enforcement action pursuant to this section.

(c) The commissioner may, after notice and an opportunity for hearing, issue an order requiring an institution to cease and desist from any violation or unsafe or unsound practice. The commissioner shall serve to the institution a written notice describing the alleged violation or practice and specifying a time and place for a hearing to be held at which the institution may present evidence or argument. The hearing shall be held no later than fifteen days after the notice has been issued by the commissioner. If, after the hearing, the commissioner finds that the institution has engaged in the alleged conduct, the commissioner may issue a cease and desist order for the

institution to immediately discontinue the specified conduct and take affirmative action necessary to prevent its recurrence.

(d) If the commissioner finds that an institution's conduct or condition is likely to cause immediate and irreparable harm to is customers or the public before a formal hearing can be concluded, the commissioner may issue a temporary emergency order. The order may direct the institution to immediately cease or refrain from a specified activity, or to take any other action necessary to prevent or mitigate future harm. A temporary emergency order shall be effective upon service on the institution. An institution subject to a temporary emergency order shall be given the opportunity for an expedited hearing. Upon the institution's request, a hearing shall be held no later than ten days after the commissioner issues an emergency order. Following the hearing, the commissioner may stay, modify, or make permanent the order. If no hearing is requested within ten days or if the institution fails to appear at the scheduled hearing, the temporary order shall remain in effect until the commissioner lifts or replaces the order.

(e) The commissioner may impose civil monetary penalties for violations of this part. For the first offense, the penalty shall not exceed $5,000 per violation. For each subsequent offense, the penalty shall not exceed $10,000 per violation. Each act or omission that is found to violate this part shall be considered a separate violation for the purposes of assessing civil penalties. The commissioner shall issue a written notice to the institution identifying the violation and the amount of the penalty and informing the institution of its right to request an administrative hearing on the penalty in accordance with subsection (g).

(f) If, after notice and an opportunity for a hearing, the commissioner finds that an institution has committed a violation of this part, has defied an order issued by the commissioner, or is conducting its digital asset services in a manner that poses a significant risk to the safety of customer assets or to the soundness of the institution, the commissioner may suspend or revoke the institution's authority to provide digital asset services pursuant to this part. Any notice of intent to suspend or revoke an institution's authority under this part shall state the grounds for the action and set a date for a hearing at which

the institution may show cause as to why its authority should not be suspended or revoked. Any suspension or revocation issued pursuant to this subsection shall become effective only after the institution has been given notice, an opportunity for a hearing, and a written decision by the commissioner affirming grounds for the action.

(g) An institution subject to any final enforcement action, including a cease and desist order, temporary emergency order, civil penalty, or suspension or revocation, may request an administrative hearing and judicial review of the commissioner's decision. Upon timely request by the institution, the commissioner shall conduct an administrative hearing no later than seven days after the institution's request has been received. The institution may present evidence and argument at the hearing, and the commissioner shall issue a written final decision based on the record of the proceedings. An institution may appeal a final decision of the commissioner to a court of competent jurisdiction as provided by law. The filing of an appeal shall operate as an automatic stay of the commissioner's order, unless the court, upon motion of the commissioner, finds that the stay would pose a substantial risk

to the public interest. Any appeal filed under this subsection shall be expedited and given priority on the court's docket. The reviewing court shall hear and determine the appeal as promptly as practicable, giving precedence over other civil matters, except matters of the same character.

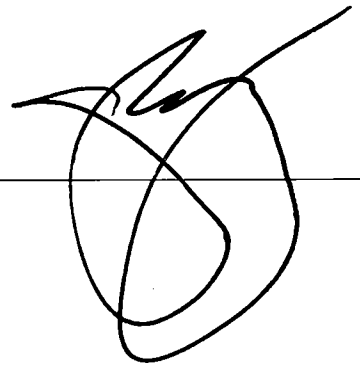
**§412:3-H Construction; applicability.** Nothing in this part shall be construed to alter, diminish, or expand the duties and obligations of banks, credit unions, or fiduciaries under existing state or federal law, except as expressly provided in this part."

SECTION 3. If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the invalidity does not affect other provisions or applications of the Act that can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable.

SECTION 4. In codifying the new sections added by section 2 of this Act, the revisor of statutes shall substitute appropriate section numbers for the letters used in designating the new sections in this Act.

SECTION 5. This Act shall take effect on September 1, 2026.

INTRODUCED BY: _____



# S.B. NO. 3184

**Report Title:**
DFI; Digital Asset Banking; Financial Institutions; Regulation

**Description:**
Authorizes digital asset banking in the State. Requires the Commissioner of Financial Institutions to adopt and enforce regulations for digital asset banking. Effective 9/1/2026.

*The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.*