State of Arkansas *As Engrossed: H3/11/25 H3/17/25*
95th General Assembly **A Bill**
Regular Session, 2025 HOUSE BILL 1467

By: Representatives Achor, *McCollum*
By: Senator J. Boyd

For An Act To Be Entitled

AN ACT TO AMEND THE UNIFORM MONEY SERVICES ACT; AND FOR OTHER PURPOSES.

Subtitle

TO AMEND THE UNIFORM MONEY SERVICES ACT.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

SECTION 1. Arkansas Code § 23-55-102, concerning the definitions used under the Uniform Money Services Act, is amended to add additional subdivisions to read as follows:

(24) "Elder adult" means a person who is sixty years of age or older.

(25) "Existing customer" means a consumer who:

(A) is engaging in a transaction at a virtual currency kiosk in the state; and

(B) has been registered for more than seventy-two hours as a customer of the:

(i) owner of the virtual currency kiosk; or

(ii) virtual currency kiosk operator.

(26)(A) "Money transmission kiosk" or “virtual currency kiosk” means an automated, unstaffed electronic machine that allows users to engage in money transmission, including any machine that is capable of accepting or dispensing cash in exchange for virtual currency.

(B) "Money transmission kiosk" or "virtual currency kiosk" does not include consumer cellular telephones and other similar personal devices.

(27) "New customer" means a consumer who:

(A) is engaging in a transaction at a virtual currency kiosk in this state; and

(B) has been registered for less than seventy-two hours as a customer of the:

(i) owner of the virtual currency kiosk; or

(ii) virtual currency kiosk operator.

(28) "Unique identifier" means a number or other identifier that is assigned by a protocol established by the automated licensing system approved by the commissioner.

(29) "Virtual currency kiosk operator" means a person that engages in virtual currency business activity through a money transmission kiosk located in this state or a person that owns, operates, or manages a money transmission kiosk located in this state through which virtual currency business activity is offered.

(30) "Virtual currency storage" means:

(A) maintaining possession, custody, or control over virtual currency on behalf of another person, including as a virtual currency control-services vendor;

(B) issuing, transferring, or otherwise granting or providing to any person in this State any claim or right or any physical, digital, or electronic instrument, receipt, certificate, or record representing any claim or right to receive, redeem, withdraw, transfer, exchange, or control any virtual currency or amount of virtual currency; or

(C) receiving possession, custody, or control over virtual currency from a person in this State in return for a promise or obligation to return, repay, exchange, or transfer such virtual currency or a like amount of such virtual currency.

(31) "Virtual currency wallet" means a software application or other mechanism providing a means for holding, storing, and transferring virtual currency.

SECTION 2. Arkansas Code § 23-55-202(b)(4), concerning the application for a license under the Uniform Money Services Act, is amended to read as follows:

(4) a list of the applicant's proposed authorized delegates and

the locations, including money transmission kiosks and virtual currency kiosks, located in this State where the applicant and its authorized delegates propose to engage in money transmission or provide other money services;

SECTION 3. Arkansas Code § 23-55-204 is amended to read as follows:

23-55-204. Surety bonds.

(a) An applicant for a money transmission license shall provide, and a licensee at all times shall maintain, security consisting of a surety bond ~~in a form satisfactory to the Securities Commissioner~~.

(b)(1) The surety bond under subsection (a) shall be in a form satisfactory to the Securities Commissioner and shall run to the State of Arkansas for the benefit of any claimants against the licensee to secure the faithful performance of the obligations of the licensee with respect to the receipt, handling, transmission, and payment of money in connection with money transmission.

(2) The commissioner has the discretion to require the applicant to obtain additional security coverage to address related cybersecurity risks inherent in the applicant's business model as it relates to virtual currency transmission and to the extent the risks are not within the scope of the required surety bond.

(c) The amount of the required security under this section shall be:

(1) the greater of $100,000 or an amount equal to 100 percent of the licensee's average daily money transmission liability in this state, calculated for the most recently completed three-month period, up to a maximum of $500,000; or

(2) if the licensee's tangible net worth exceeds 10 percent of total assets, then the licensee shall maintain a surety bond of $100,000.

~~(c)~~(d) A licensee that maintains a bond in the maximum amount provided for in ~~subsection (b)~~ subsection (c), as applicable, is not required to calculate its average daily money transmission liability in this state for purposes of § 23-55-702.

~~(d)~~(e) A licensee may exceed the maximum required bond amount under § 23-55-702(a)(6).

(f)(1) A party having a claim against the licensee may bring suit directly on the surety bond, or the commissioner may bring suit on behalf of

any claimants, either in one action or in successive actions.

(2) Consumer claims shall be given priority in recovering from the surety bond.

(3) Every bond shall provide for suit on the surety bond by a person who has a cause of action under this subchapter.

(g)(1) The surety bond shall remain in effect until cancellation, which may occur only after sixty days' written notice to the commissioner.

(2) Cancellation shall not affect any liability incurred or accrued during that period.

(h)(1) Except as provided by subdivision (h)(2), the surety bond shall remain in place for no less than five (5) years after the licensee ceases money transmission operations in this state.

(2) The commissioner may permit the surety bond to be reduced or eliminated before that time to the extent that the amount of the licensee's outstanding payment instruments, stored value obligations, and money transmitted in this state is reduced.

SECTION 4. Arkansas Code § 23-55-404(b), concerning the renewal of a currency exchange license under the Uniform Money Services Act, is amended to read as follows:

(b) A licensee under this article shall submit a renewal report with the renewal fee, in a form and in a medium prescribed by the commissioner. The renewal report must contain a list of the locations in this State where the licensee or an authorized delegate of the licensee engages in currency exchange, including limited stations, ~~and~~ mobile locations, money transmission kiosks, and virtual currency kiosks.

SECTION 5. Arkansas Code § 23-55-501(b), concerning a contract between a licensee and an authorized delegate under the Uniform Money Services Act, is amended to read as follows:

(b)(1) A contract between a licensee and an authorized delegate must require the authorized delegate to operate in full compliance with this chapter.

(2)(A) The licensee shall furnish in a record to each authorized delegate policies and procedures sufficient for compliance with this chapter.

(B) The policies and procedures under subdivision

(b)(2)(A) shall be updated on a reasonably periodic basis.

SECTION 6. Arkansas Code § 23-55-501, concerning the relationship between a licensee and an authorized delegate under the Uniform Money Services Act, is amended to add an additional subsection to read as follows:

(g) A copy of a contract required under this section shall be made available to the Securities Commissioner, upon request.

SECTION 7. Arkansas Code Title 23, Chapter 55, Subchapter 5, is amended to add an additional section to read as follows:

23-55-503. Training materials provided to authorized delegates.

(a) On or before April 1 of each year, a licensee shall provide to each authorized delegate through which it engages in the business of money transmission training materials on how to:

(1) recognize financial abuse and financial exploitation of an elder adult; and

(2) respond appropriately if the authorized delegate suspects that the authorized delegate is being asked to engage in the business of money transmission for a fraudulent transaction in which an elder adult is the victim of financial abuse or financial exploitation.

(b) A licensee shall provide the training materials required under subsection (a) to each newly appointed authorized delegate within one month after appointment of the authorized delegate.

SECTION 8. Arkansas Code § 23-55-603(b), concerning a list of authorized delegates required under the Uniform Money Services Act, is amended to read as follows:

(b) A licensee shall file with the commissioner within 45 days after the end of each calendar quarter a current list of all authorized delegates, and locations in this State where the licensee or an authorized delegate of the licensee provides money services, including limited stations, ~~and~~ mobile locations, money transmission kiosks, and virtual currency kiosks. The licensee shall state the name and street address of each location and authorized delegate.

SECTION 9. Arkansas Code § 23-55-608, concerning disclosure

requirements under the Uniform Money Services Act, is amended to add an additional subsection to read as follows:

(c)(1) Except as required by § 23-55-1008(a), a licensee or authorized delegate shall include a clear, concise, and conspicuous fraud warning that is posted in a conspicuous area or included on a transmittal form used by a consumer to send money to another individual.

(2) The fraud warning required under subdivision (c)(1) shall:

(A) include a toll-free telephone number for consumers to call to report fraud or suspected fraud; and

(B) be in clear, conspicuous, and legible writing in English and in the language principally used by the licensee or authorized delegate to advertise, solicit, or negotiate, either orally or in writing, for a transaction conducted in person, electronically, or by telephone, if other than English.

(3) A licensee shall monitor the activities of its authorized delegates relating to transmittals by consumers.

(4) If a licensee or authorized delegate conducts money transmission activity through a website or a mobile application that is not in a physical location, the commissioner may authorize an alternative form of the fraud notice required under subdivision (c)(1).

SECTION 10. Arkansas Code Title 23, Chapter 55, Subchapter 10, is amended to add an additional section to read as follows:

23-55-1008. Virtual currency kiosk requirements.

(a)(1) The owner of a virtual currency kiosk or a virtual currency kiosk operator, in establishing a relationship with a customer and before entering into an initial virtual currency transaction on behalf of or with the customer, shall disclose in clear, conspicuous, and legible writing in English and in the language principally used by the licensee or authorized delegate to advertise, solicit, or negotiate, either orally or in writing, for a transaction conducted in person, electronically, or by phone, if other than English, all material risks associated with virtual currency generally.

(2) The material risks associated with virtual currency required to be disclosed under subdivision (a)(1) include without limitation:

(A) a disclosure that is acknowledged by the customer and provided separately from the disclosures provided under subdivision (a)(2)(B)

and subdivision (a)(2)(G), and written prominently and in bold type, stating the following:

"WARNING: LOSSES DUE TO FRAUDULENT OR ACCIDENTAL TRANSACTIONS MAY NOT BE RECOVERABLE AND TRANSACTIONS IN VIRTUAL CURRENCY ARE IRREVERSIBLE.";

(B) virtual currency is not backed or insured by the government and accounts and value balances are not subject to protections of the Federal Deposit Insurance Corporation, National Credit Union Administration, or Securities Investor Protection Corporation;

(C) a virtual currency transaction may be deemed to be made when recorded on a public ledger which may not be the date or time when the customer initiates the virtual currency transaction;

(D) the value of virtual currency may be derived from the continued willingness of market participants to exchange fiat currency for virtual currency which may result in the permanent and total loss of the value of a particular virtual currency if the market for that virtual currency disappears;

(E) the volatility and unpredictability of the price of virtual currency relative to fiat currency may result in a significant loss over a short period of time;

(F) a bond maintained by the owner of a virtual currency kiosk or a virtual currency kiosk operator for the benefit of the customers of the owner of a virtual currency kiosk or a virtual currency kiosk operator may not be sufficient to cover all losses incurred by customers; and

(G)(i) virtual currency transactions are irreversible and may be used by a person seeking to defraud customers.

(ii) As used in subdivision (a)(2)(G)(i), "seeking to defraud customers" includes without limitation a person:

(a) impersonating a customer's family or friends;

(b) threatening jail time;

(c) stating that a customer's identity has been stolen;

(d) insisting that a customer withdraw money from the customer's bank account and purchase virtual currency; or

(e) alleging that a customer's personal computer has been hacked.

(b)(1) An owner of a virtual currency kiosk or a virtual currency kiosk operator, when opening an account for a new customer and before entering into an initial virtual currency transaction for, on behalf of, or with the customer, shall disclose in clear, conspicuous, and legible writing in English and in the language principally used by the licensee or authorized delegate to advertise, solicit, or negotiate, either orally or in writing, for a transaction conducted in person, electronically, or by phone, if other than English, using not less than twenty-four point sans-serif-type font, all relevant terms and conditions associated with the products, services, and activities of the owner of a virtual currency kiosk or a virtual currency kiosk operator and virtual currency generally.

(2) The disclosure required under subdivision (b)(1) shall include without limitation:

(A) the customer's liability for unauthorized virtual currency transactions;

(B) the customer's right to stop payment of a preauthorized virtual currency transfer and the procedure used to initiate a stop-payment order;

(C) the circumstances under which the owner of a virtual currency kiosk or a virtual currency kiosk operator, absent a court or government order, will disclose information concerning the customer's account to third parties;

(D) the requirement that the owner of a virtual currency kiosk or a virtual currency kiosk operator communicate to the customer what customer information may be disclosed to third parties;

(E) the customer's right to receive a receipt for a virtual currency transaction at the time of the transaction;

(F) upon a change in the rules or policies of the owner or operator, the customer's right to consent to the changed rules or policies before performing a transaction after the change; and

(G) any other disclosures that are customarily provided in connection with opening a person's account.

(c)(1) An owner of a virtual currency kiosk or a virtual currency kiosk operator, before each transaction in virtual currency for, on behalf of, or with a customer, shall disclose to the customer in an easily readable manner that is in clear, conspicuous, and legible writing in English and in

the language principally used by the licensee or authorized delegate to advertise, solicit, or negotiate, either orally or in writing, for a transaction conducted in person, electronically, or by phone, if other than English, using not less than twenty-four point sans-serif-type font, the terms and conditions of the virtual currency transaction.

(2) The terms and conditions required under subdivision (c)(1) shall include without limitation:

(A) the amount of the transaction;

(B) any fees, expenses, and charges borne by the customer, including without limitation applicable exchange rates;

(C) the type and nature of the virtual currency transaction;

(D) a warning that, once executed, the virtual currency transaction may not be undone, if applicable;

(E) a daily virtual currency transaction limit according to subsection (g);

(F) the difference in the sale price of the virtual currency versus the current market price; and

(G) any other disclosures that are customarily given in connection with a virtual currency transaction.

(d) An owner of a virtual currency kiosk or a virtual currency kiosk operator shall ensure that each customer acknowledges receipt of all disclosures required under this section.

(e)(1) An owner of a virtual currency kiosk or a virtual currency kiosk operator, upon the completion of a virtual currency transaction, shall provide to the customer a receipt containing:

(A) the name of, and contact information for, the owner of the virtual currency kiosk or the virtual currency kiosk operator, including without limitation the owner of the virtual currency kiosk's or the virtual currency kiosk operator's business address and a customer service telephone number established by the owner of a virtual currency kiosk or the virtual currency kiosk operator to answer questions and register complaints;

(B) the name of the customer;

(C) the type, value, date and precise time of the virtual currency transaction, transaction hash or identification number, and each virtual currency address;

(D) the amount of the virtual currency transaction expressed in United States currency;

(E) the public virtual currency address of the customer;

(F) the unique identifier of the virtual currency kiosk operator;

(G) a fee charged, including without limitation a fee charged directly or indirectly by the owner of the virtual currency kiosk or the virtual currency kiosk operator, or a third party involved in the virtual currency transaction;

(H) the exchange rate, if applicable;

(I) any tax collected by the owner of the virtual currency kiosk or the virtual currency kiosk operator for the virtual currency transaction;

(J) a statement of the liability of the owner of the virtual currency kiosk or the virtual currency kiosk operator for nondelivery or delayed delivery;

(K) a statement of the refund policy of the owner of the virtual currency kiosk or the virtual currency kiosk operator;

(L) the name and telephone number of the State Securities Department and a statement disclosing that the owner of the virtual currency kiosk's or the virtual currency kiosk operator's customers may contact the department with questions or complaints about the owner of the virtual currency kiosk's or the virtual currency kiosk operator's virtual currency kiosk services; and

(M) any additional information the commissioner may require.

(2) The receipt required under subdivision (e)(1):

(A) shall be provided in:

(i) a retainable form;

(ii) English; and

(iii) the language principally used by the owner of the virtual currency kiosk or the virtual currency kiosk operator to advertise, solicit, or negotiate, orally or in writing; and

(B) may be provided electronically if the customer requests or agrees to receive an electronic receipt.

(f) The total amount of a fee and commission charged by an owner of

the virtual currency kiosk or a virtual currency kiosk operator for a virtual currency transaction shall not exceed:

(1) five dollars; or

(2) *eighteen percent* of the amount of the virtual currency transaction.

(g) There are established the following maximum daily virtual currency kiosk transaction limits:

(1) two thousand dollars for each new customer of a virtual currency kiosk; and

(2) *seven thousand five hundred dollars* for each existing customer of a virtual currency kiosk.

(h) The owner of a virtual currency kiosk or a virtual currency kiosk operator shall allow a new customer, upon the request of the new customer, to cancel and receive a full refund for any fraudulent virtual currency transactions that occurred not later than seventy-two hours after the new customer registered as a customer of the owner of the virtual currency kiosk or the virtual currency kiosk operator if, not later than *fourteen days* after the last virtual currency transaction that occurred during the seventy-two hour period, the new customer:

(1) contacts the owner of the virtual currency kiosk or the virtual currency kiosk operator and a government or law enforcement agency to inform the owner of the virtual currency kiosk or the virtual currency kiosk operator and government or law enforcement agency of the fraudulent nature of the virtual currency transaction; and

(2) files a report with a government or law enforcement agency memorializing the fraudulent nature of the virtual currency transaction.

(i) Each owner of a virtual currency kiosk or a virtual currency kiosk operator shall:

(1) obtain a copy of a government-issued identification card that identifies each customer of the owner of the virtual currency kiosk or the virtual currency kiosk operator;

(2) maintain restrictions that prevent more than one customer of the owner of the virtual currency kiosk or the virtual currency kiosk operator from using the same virtual currency wallet;

(3) be able to prevent designated virtual currency wallets from being used at a virtual currency kiosk owned or operated by the owner of the

virtual currency kiosk or the virtual currency kiosk operator;

(4) use an established third party that specializes in performing blockchain analyses to preemptively perform the analyses to identify and prevent high risk or sanctioned virtual currency wallets from being used by customers at virtual currency kiosks owned or operated by the owner of the virtual currency kiosk or the virtual currency kiosk operator;

(5) define, in the owner of the virtual currency kiosk's or the virtual currency kiosk operator's policies and procedures, a risk-based method of monitoring customers of the owner of the virtual currency kiosk or the virtual currency kiosk operator on a post-transaction basis;

(6) offer, during the hours of operation of the virtual currency kiosks owned or operated by the owner of the virtual currency kiosk or the virtual currency kiosk operator, live customer support by telephone from a telephone number prominently displayed at or on the virtual currency kiosks;

(7)(A) identify and speak by telephone with an elder adult who is a new customer before the elder adult who is a new customer completes his or her first virtual currency transaction with the owner of the virtual currency kiosk or the virtual currency kiosk operator.

(B) During the communication, which shall be recorded and retained by the owner of the virtual currency kiosk or the virtual currency kiosk operator, the owner of the virtual currency kiosk or the virtual currency kiosk operator shall:

(i) reconfirm any attestations made by the new customer at a virtual currency kiosk owned or operated by the owner of the virtual currency kiosk or the virtual currency kiosk operator;

(ii) discuss the transaction; and

(iii)(a) discuss types of fraudulent schemes relating to virtual currency.

(b) The owner of the virtual currency kiosk's or the virtual currency kiosk operator's approval of the transaction shall be dependent upon the owner of the virtual currency kiosk's or the virtual currency kiosk operator's assessment of the communication;

(8) designate and employ a chief compliance officer who shall:

(A) be qualified to coordinate and monitor a compliance program to ensure compliance with this section and all other applicable federal laws and regulations and state laws and rules; and

(B) not own more than twenty percent of the owner of the virtual currency kiosk or the virtual currency kiosk operator that employs the officer; and

(9) use full-time employees to fulfill the owner of the virtual currency kiosk's or the virtual currency kiosk operator's compliance responsibilities under federal laws and regulations and state laws and rules.

SECTION 11. Arkansas Code Title 23, Chapter 55, is amended to add an additional subchapter to read as follows:

Article 11 — Data Security for Money Services

23-55-1101. Definitions.

In this subchapter:

(1) "Authorized user" means an employee, contractor, agent, or other person that participates in a financial institution's business operations and is authorized to access and use a financial institution's information systems and data.

(2) "Consumer" means an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

(3) "Customer" means a consumer who has a customer relationship with a financial institution.

(4) "Customer information" means a record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of a financial institution or the financial institution's affiliates.

(5) "Customer relationship" means a continuing relationship between a consumer and a financial institution under which the financial institution provides to the consumer one or more financial products or services that are used primarily for personal, family, or household purposes.

(6) "Encryption" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

(7) "Financial institution" means a money services business licensed under this chapter.

(8)(A) "Financial product or service" means a product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. § 1843(k), as it existed on January 1, 2025.

(B) "Financial product or service" includes a financial institution's evaluation or brokerage of information that a financial institution collects in connection with a request or an application from a consumer for a financial product or service.

(9) "Information security program" means the administrative, technical, or physical safeguards a financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(10) "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, including any specialized system such as industrial controls systems or process controls systems, telephone switching and private branch exchange systems, and environmental controls systems, that contains customer information or that is connected to a system that contains customer information.

(11) "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:

(A) knowledge factors, including without limitation a password;

(B) possession factors, including without limitation a token; or

(C) inherence factors, including without limitation biometric characteristics.

(12)(A) "Nonpublic personal information" means:

(i) personally identifiable financial information; and

(ii) a list, description, or other grouping of consumers, and publicly available information pertaining to a consumer, that

is derived using personally identifiable financial information that is not publicly available.

(B) "Nonpublic personal information" includes without limitation a list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available.

(C) "Nonpublic personal information" does not include:

(i) publicly available information except as included on a list described in subdivision (12)(A)(ii);

(ii) a list, description, or other grouping of consumers, and publicly available information pertaining to the list, description, or other grouping of consumers, that is derived without using personally identifiable financial information that is not publicly available; or

(iii) a list of individuals' names and addresses that contains only publicly available information and is not:

(a) derived, in whole or in part, using personally identifiable financial information that is not publicly available; and

(b) disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(13)(A) "Notification event" means acquisition of unencrypted customer information without the authorization of an individual to which the information pertains.

(B) For purposes of subdivision (13)(A):

(i) customer information is considered unencrypted if the encryption key was accessed by an unauthorized person; and

(ii) unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless a financial institution has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of the customer information.

(14) "Penetration testing" means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside a financial institution's information systems.

(15)(A) "Personally identifiable financial information" means information:

(i) a consumer provides to a financial institution to obtain a financial product or service from a financial institution;

(ii) about a consumer resulting from a transaction involving a financial product or service between a financial institution and a consumer; or

(iii) a financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.

(B) "Personally identifiable financial information" includes:

(i) information a consumer provides to a financial institution on an application to obtain a loan, credit card, or other financial product or service;

(ii) account balance information, payment history, overdraft history, and credit or debit card purchase information;

(iii) the fact that an individual is or has been a financial institutions' customer or has obtained a financial product or service from a financial institution;

(iv) information about a financial institution's consumer if the information is disclosed in a manner that indicates that the individual is or has been the financial institution's consumer;

(v) information that a consumer provides to a financial institution or that a financial institution or a financial institution's agent otherwise obtains in connection with collecting on, or servicing, a credit account;

(vi) information a financial institution collects through an internet cookie or the information collecting device from a computer server; and

(vii) information from a consumer report.

(C) "Personally identifiable financial information" does not include:

(i) a list of names and addresses of customers of an entity that is not a financial institution; and

(ii) information that does not identify a consumer,

including aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(16)(A) "Publicly available information" means information that a financial institution has a reasonable basis to believe is lawfully made available to the public from:

(i) federal, state, or local government records;

(ii) widely distributed media; or

(iii) disclosures to the public that are required to be made by federal, state, or local law.

(B) "Publicly available information" includes without limitation:

(i) information in government records, including information in government real estate records and security interest filings; and

(ii)(a) information from widely distributed media, including information from a telephone book, a television or radio program, a newspaper, or a website that is available to the public on an unrestricted basis.

(b) A website is not restricted under subdivision (16)(B)(ii)(a) merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the public.

(C) For purposes of this subdivision (16), a financial institution has a reasonable basis to believe that:

(i) information is lawfully made available to the public if the financial institution has taken steps to determine:

(a) that the information is of the type that is available to the public; and

(b) whether an individual can direct that the information not be made available to the public and, if so, that the financial institution's consumer has not directed that the information not be made available to the public;

(ii) mortgage information is lawfully made available to the public if the financial institution determines that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded; and

(iii) an individual's telephone number is lawfully made available to the public if the financial institution has located the telephone number in a telephone directory or the consumer has informed the financial institution that the telephone number is not unlisted.

(17) "Qualified individual" means an individual designated by a financial institution to oversee, implement, and enforce the financial institution's information security program.

(18) "Security event" means an event resulting in unauthorized access to, or disruption or misuse of:

(A) an information system or information stored on the information system; or

(B) customer information held in physical form.

(19) "Service provider" means a person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this subchapter.

23-55-1102. Standards for safeguarding customer information.

(a) A financial institution shall develop, implement, and maintain a comprehensive information security program.

(b) The information security program under subsection (a) of this section shall:

(1) be written in one or more readily accessible parts; and

(2) contain administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of the financial institution's activities, and the sensitivity of any customer information at issue.

(c) The information security program shall include the information required under § 23-55-1103.

23-55-1103. Information security program required elements.

(a) In order for a financial institution to develop, implement, and maintain an information security program, the financial institution shall comply with this section.

(b)(1) A financial institution shall designate a qualified individual responsible for overseeing and implementing the financial institution's

information security program and enforcing an information security program.

(2)(A) The qualified individual may be employed by the financial institution, an affiliate, or a service provider.

(B) If a financial institution designates an individual employed by an affiliate or service provider, the financial institution shall:

(i) retain responsibility for compliance with this section;

(ii) designate a senior member of the financial institution's personnel to be responsible for direction and oversight of the qualified individual; and

(iii) require the service provider or affiliate to maintain an information security program that protects the financial institution in accordance with the requirements of this section.

(c)(1) A financial institution shall base the financial institution's information security program on a risk assessment that:

(A) identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the information; and

(B) assesses the sufficiency of any safeguards in place to control these risks.

(2) The risk assessment shall be written and include:

(A) criteria for the evaluation and categorization of identified security risks or threats the financial institution faces;

(B) criteria for the assessment of the confidentiality, integrity, and availability of the financial institution's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats the financial institution faces; and

(C) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(3) A financial institution shall periodically perform additional risk assessments that:

(A) reexamine the reasonably foreseeable internal and

external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information; and

(B) reassess the sufficiency of any safeguards in place to control these risks.

(d) A financial institution shall design and implement safeguards to control the risks the financial institution identifies through the risk assessment as required under subsection (c), including without limitation:

(1) implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls, to:

(A) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(B) limit authorized users' access only to customer information that the authorized user needs to perform the authorized user's duties and functions, or in the case of customers, to access the customer's own customer information;

(2) identifying and managing the data, personnel, devices, systems, and facilities that enable the financial institution to achieve business purposes according to the financial institution's relative importance to business objectives and the financial institution's risk strategy;

(3)(A) protecting by encryption all customer information held or transmitted by the financial institution both in transit over external networks and at rest.

(B) to the extent the financial institution determines that encryption of customer information, either in transit over external networks or at rest, is infeasible, the financial institution may instead secure the customer information using effective alternative compensating controls reviewed and approved by the financial institution's qualified individual;

(4) adopting secure development practices for in-house developed applications utilized by the financial institution for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications the financial institution utilizes to transmit, access, or store customer

information;

(5) implementing multi-factor authentication for an individual accessing an information system, unless the financial institution's qualified individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6) developing, implementing, and maintaining procedures for the secure disposal of customer information in any format no later than two years after the last date the customer information is used in connection with the provision of a financial product or service to the customer, unless the customer information is:

(A) necessary for business operations or for other legitimate business purposes;

(B) otherwise required to be retained by state law or rule, or federal law or regulation; or

(C) where targeted disposal is not reasonably feasible due to the manner in which the information is maintained;

(7) periodically reviewing the financial institution's data retention policy to minimize the unnecessary retention of data;

(8) adopting procedures for change management; and

(9) implementing policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by these users.

(e)(1) A financial institution shall regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures of the safeguards required under this section, including those to detect actual and attempted attacks on or intrusions into information systems.

(2)(A) For information systems, monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments.

(B) Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the financial institution shall conduct:

(i) annual penetration testing of a financial institution's information systems determined each given year based on relevant identified risks according to the risk assessment; and

(ii) vulnerability assessments, including a systemic scan or review of an information system reasonably designed to identify publicly known security vulnerabilities in the financial institution's information systems based on the risk assessment, at least every six months, and whenever there are:

(a) material changes to the financial institution's operations or business arrangements; and

(b) circumstances the financial institution knows or has reason to know may have a material impact on the financial institution's information security program.

(f) A financial institution shall implement policies and procedures to ensure that personnel are able to enact the financial institution's information security program by:

(1) providing the financial institution's personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) utilizing qualified information security personnel employed by the financial institution or an affiliate or service provider sufficient to manage the financial institution's information security risks and to perform or oversee the information security program;

(3) providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(g) A financial institution shall oversee service providers by:

(1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

(2) requiring the financial institution's service providers by contract to implement and maintain the safeguards referenced under subdivision (g)(1); and

(3) periodically assessing the financial institution's service providers based on the risk they present and the continued adequacy of their safeguards.

(h) A financial institution shall evaluate and adjust the financial

institution's information security program to reflect:

(1) the results of the testing and monitoring required by subsection (e);

(2) upon any material change to the financial institution's operations or business arrangements or other circumstances;

(3) the results of risk assessments performed under subdivision (c)(3); and

(4) any other circumstances that the financial institution knows or has reason to know may have a material impact on the financial institution's information security program.

(i)(1) A financial institution shall establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in the financial institution's control.

(2) The incident response plan under subdivision (i)(1) shall address:

(A) the goals of the incident response plan;

(B) the internal processes for responding to a security event;

(C) the definition of clear roles, responsibilities, and levels of decision-making authority;

(D) external and internal communications and information sharing;

(E) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(F) documentation and reporting regarding security events and related incident response activities; and

(G) the evaluation and revision as necessary of the incident response plan following a security event.

(j)(1) The financial institution's qualified individual shall report in writing at least annually, to the financial institution's board of directors or equivalent governing body.

(2) If a board of directors or equivalent governing body does not exist, the report required under subdivision (j)(1) shall be timely presented to a senior officer responsible for the financial institution's information security program.

(3) The report required under subdivision (j)(1) shall include:

(A) the overall status of the information security program and the financial institution's compliance with this section and associated rules; and

(B) material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses to security events or violations, and recommendations for changes in the information security program.

(k) A financial institution shall provide notice to the Securities Commissioner about notification events according to subdivisions (l)(1) and (2).

(l)(1) Upon discovery of a notification event as described in subdivision (l)(2), if the notification event involves the information of any consumers in this state, the financial institution shall notify the commissioner as soon as possible, and no later than forty-five days after discovery of the notification event.

(2) The notice required under subdivision (l)(1) shall:

(A) be made in a format specified by the commissioner; and

(B) include the following information:

(i) the name and contact information of the reporting financial institution;

(ii)(a) a description of the types of information that were involved in the notification event.

(b) if the information is possible to determine under subdivision (l)(2)(B)(ii)(a), the notice required under subdivision (l)(1) shall contain the date or date range of the notification event;

(iii) the number of consumers affected or potentially affected by the notification event;

(iv) a general description of the notification event; and

(v)(a) whether a law enforcement official has provided the financial institution with a written determination that notifying the public of the notification event would impede a criminal

investigation or cause damage to national security, and a means for the commissioner to contact the law enforcement official.

(b) A law enforcement official under subdivision (l)(2)(B)(v)(a) may request an initial delay of up to thirty days following the date when notice was provided to the commissioner.

(c) The delay under subdivision (l)(2)(B)(v)(b) may be extended for an additional period of up to sixty days if the law enforcement official seeks an extension in writing.

(d) An additional delay beyond the delay under subdivision (l)(2)(B)(v)(b) may be permitted only if the State Securities Department determines that public disclosure of a notification event continues to impede a criminal investigation or cause damage to national security.

(3)(A) A notification event under this section shall be treated as discovered as of the first day on which the notification event is known to the financial institution.

(B) The financial institution under subdivision (l)(3)(A) shall be deemed to have knowledge of a notification event if the notification event is known to a person, other than the person committing the notification event, who is the financial institution's employee, officer, or other agent.

(m) A financial institution shall establish a written plan addressing business continuity and disaster recovery.

23-55-1104. Exceptions.

This article does not apply to a financial institution that maintains customer information concerning fewer than five thousand consumers.

/s/Achor