

1 State of Arkansas
2 95th General Assembly
3 Regular Session, 2025
4

As Engrossed: H3/11/25

A Bill

HOUSE BILL 1467

5 By: Representative Achor
6 By: Senator J. Boyd
7

For An Act To Be Entitled

9 AN ACT TO AMEND THE UNIFORM MONEY SERVICES ACT; AND
10 FOR OTHER PURPOSES.
11

Subtitle

12 TO AMEND THE UNIFORM MONEY SERVICES ACT.
13

14 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:
15

16 SECTION 1. Arkansas Code § 23-55-102, concerning the definitions used
17 under the Uniform Money Services Act, is amended to add additional
18 subdivisions to read as follows:
19

20 (24) "Elder adult" means a person who is sixty years of age or
21 older.
22

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

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

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

28 (i) owner of the virtual currency kiosk; or

29 (ii) virtual currency kiosk operator.

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

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



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

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

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

6 (i) owner of the virtual currency kiosk; or

7 (ii) virtual currency kiosk operator.

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

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

16 (30) "Virtual currency storage" means:

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

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

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

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

32
33 SECTION 2. Arkansas Code § 23-55-202(b)(4), concerning the application
34 for a license under the Uniform Money Services Act, is amended to read as
35 follows:

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

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

5
6 SECTION 3. Arkansas Code § 23-55-204 is amended to read as follows:

7 23-55-204. Surety bonds.

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

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

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

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

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

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

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

33 ~~(d)(e)~~ A licensee may exceed the maximum required bond amount under §
34 23-55-702(a)(6).

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

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

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

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

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

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

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

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

17
18 SECTION 4. Arkansas Code § 23-55-404(b), concerning the renewal of a
19 currency exchange license under the Uniform Money Services Act, is amended to
20 read as follows:

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

27
28 SECTION 5. Arkansas Code § 23-55-501(b), concerning a contract between
29 a licensee and an authorized delegate under the Uniform Money Services Act,
30 is amended to read as follows:

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

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

36 (B) The policies and procedures under subdivision

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

2
3 SECTION 6. Arkansas Code § 23-55-501, concerning the relationship
4 between a licensee and an authorized delegate under the Uniform Money
5 Services Act, is amended to add an additional subsection to read as follows:

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

8
9 SECTION 7. Arkansas Code Title 23, Chapter 55, Subchapter 5, is
10 amended to add an additional section to read as follows:

11 23-55-503. Training materials provided to authorized delegates.

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

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

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

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

24
25 SECTION 8. Arkansas Code § 23-55-603(b), concerning a list of
26 authorized delegates required under the Uniform Money Services Act, is
27 amended to read as follows:

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

35
36 SECTION 9. Arkansas Code § 23-55-608, concerning disclosure

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

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

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

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

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

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

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

21
22 SECTION 10. Arkansas Code Title 23, Chapter 55, Subchapter 10, is
23 amended to add an additional section to read as follows:

24 23-55-1008. Virtual currency kiosk requirements.

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

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

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

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

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

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

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

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

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

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

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

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

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

30 (b) threatening jail time;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 (A) the amount of the transaction;

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

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

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

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

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

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

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

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

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

33 (B) the name of the customer;

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

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

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

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

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

10 (H) the exchange rate, if applicable;

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

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

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

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

25 (M) any additional information the commissioner may
26 require.

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

28 (A) shall be provided in:

29 (i) a retainable form;

30 (ii) English; and

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

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

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

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

3 (1) five dollars; or

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

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

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

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

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

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

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

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

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

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

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

1 virtual currency kiosk or the virtual currency kiosk operator;

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

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

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

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

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

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

26 (ii) discuss the transaction; and

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

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

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

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

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

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

7
8 SECTION 11. Arkansas Code Title 23, Chapter 55, is amended to add an
9 additional subchapter to read as follows:

10
11 Article 11 – Data Security for Money Services

12
13 23-55-1101. Definitions.

14 In this subchapter:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

33 (i) personally identifiable financial information;
34 and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11 (B) "Personally identifiable financial information"
12 includes:

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

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

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

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

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

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

31 (vii) information from a consumer report.

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

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

36 (ii) information that does not identify a consumer,

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

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

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

7 (ii) widely distributed media; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 (B) customer information held in physical form.

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

17
18 23-55-1102. Standards for safeguarding customer information.

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

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

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

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

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

30
31 23-55-1103. Information security program required elements.

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

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

1 information security program and enforcing an information security program.

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

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

7 (i) retain responsibility for compliance with this
8 section;

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

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

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

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

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

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

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

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

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

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

36 (A) reexamine the reasonably foreseeable internal and

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

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

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

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

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

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

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

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

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

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

1 information;

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

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

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

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

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

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

19 (8) adopting procedures for change management; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 institution's information security program to reflect:

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

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

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

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

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

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

17 (A) the goals of the incident response plan;

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

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

22 (D) external and internal communications and information
23 sharing;

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

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

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

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

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

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

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

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

11 (k) A financial institution shall provide notice to the Securities
12 Commissioner about notification events according to subdivisions (l)(1) and
13 (2).

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

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

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

21 (B) include the following information:

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

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

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

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

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

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

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

3 (b) A law enforcement official under
4 subdivision (1)(2)(B)(v)(a) may request an initial delay of up to thirty days
5 following the date when notice was provided to the commissioner.

6 (c) The delay under subdivision
7 (1)(2)(B)(v)(b) may be extended for an additional period of up to sixty days
8 if the law enforcement official seeks an extension in writing.

9 (d) An additional delay beyond the delay under
10 subdivision (1)(2)(B)(v)(b) may be permitted only if the State Securities
11 Department determines that public disclosure of a notification event
12 continues to impede a criminal investigation or cause damage to national
13 security.

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

17 (B) The financial institution under subdivision (1)(3)(A)
18 shall be deemed to have knowledge of a notification event if the notification
19 event is known to a person, other than the person committing the notification
20 event, who is the financial institution's employee, officer, or other agent.

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

23
24 23-55-1104. Exceptions.

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

27
28 */s/Achor*
29
30
31
32
33
34
35
36