New Arkansas Law Expands Consumer Fraud Protections and Imposes Strict Requirements on Crypto Kiosks

Nov 11, 2025

Categories:

Publications

Authors:

J. Dylan Grafe
Nancy Eff Presnell
William T. Repasky

Arkansas House Bill 1467 (HB1467), enacted into law in April of 2025, introduced a number of new money transmission registration and operation requirements, each of which are particularly relevant to operators of cryptocurrency kiosks.

HB1467 updates the currently enacted Arkansas Uniform Money Services Act, including adding onerous requirements for kiosk operators. Arkansas is taking a strong and broad stance to try to stop bad actors in the state from using cryptocurrency kiosks; however, this comes at the expense of money transmitters and kiosk operators who will see significant increases in compliance requirements and costs.

Generally, HB1467 implements changes which (1) establish a recission right for customers, (2) standardizes required disclosures to customers, (3) impact kiosk operators economically, and (4) require implementation of certain compliance and data security programs.

Rescission Right

Certain financial regulatory regimes require that consumers be afforded the right to rescind certain transactions for a period of time. This occurs most notably with providers of remittance transfers (i.e., a transfer of funds from a U.S. person to a non-U.S. person) where a 30-minute cancellation window must be afforded to consumers after they initiate a remittance transfer.

With HB1467, Arkansas has built a statutory requirement where new customers may be afforded a recission right if certain criteria are met which relate to the customer believing that fraud is at play. HB1467requires that kiosk operators allow new customers the right to cancel and receive a full refund for any fraudulent virtual

currency transactions that occurred not later than 72 hours after they registered as a customer of the owner or operator of the virtual currency kiosk. Refund requests must be submitted within 14 days after the last virtual currency transaction that occurred during the 72-hour period. Additionally, to exercise their recission right, new customers must: (1) contact the owner or operator of the virtual currency kiosk and a government or law enforcement agency to inform them of the fraudulent nature of the virtual currency transaction; and (2) file a report with a government or law enforcement agency memorializing the fraudulent nature of the virtual currency transaction.

This recission right poses a large operational hurdle, as kiosk operators must consider how to implement this right from a technological standpoint (building it into the machine's operating flows) and coordinate with sufficient staffing to be able to intake potential recission claims.

Disclosure Requirements

Often, kiosk operators have already adopted certain warnings and specific transaction information disclosures as part of standard kiosk operations. Arkansas HB1467, however, codifies a set of required warnings and disclosures, the latter of which may require operators to build out functionalities that allow kiosks to provide the following newly required-to-be-disclosed information to customers:

- **Pre-transaction information disclosure:** Arkansas has standardized what should be presented to a customer prior to each transaction, including: (1) the amount of the transaction; (2) any fees, expenses, and charges borne by the customer, including without limitation applicable exchange rates; (3) the type and nature of the virtual currency transaction; (4) a warning that, once executed, the virtual currency transaction may not be undone, if applicable; (5) a daily virtual currency transaction limit according to subsection (g); (6) the difference in the sale price of the virtual currency versus the current market price; and (7) any other disclosures that are customarily given in connection with a virtual currency

transaction.

- **Transaction receipt disclosures:** Arkansas has standardized what should be presented to a customer in the form of a receipt as part of each transaction. This includes: (1) the name of, and contact information for, the owner/operator of the virtual currency kiosk, including without limitation the owner's or operator's business address and a customer service telephone number established to answer questions and register complaints; (2) the name of the customer; (3) the type, value, date and precise time of the virtual currency transaction, transaction hash or identification number, and each virtual currency address; (4) the amount of the virtual currency transaction expressed in U.S. currency; (5) the public virtual currency address of the customer; (6) the unique identifier of the virtual currency kiosk operator; (7) a fee charged, including without limitation a fee charged directly or indirectly by the owner or operator of the virtual currency kiosk, or a third party involved in the virtual currency transaction; (8) the exchange rate, if applicable; (9) any tax collected by the kiosk owner/operator for the virtual currency transaction; (10) a statement of the liability of the virtual currency kiosk owner/operator for nondelivery or delayed delivery; (11) a statement of the refund policy of the virtual currency kiosk owner/operator; (12) the name and telephone number of the State Securities Department and a statement disclosing that customers of virtual currency kiosk owner/operator may contact the department with questions or complaints about kiosk services; and (13) any additional information the commissioner may require. Note that this receipt must be retainable by the customer, and it may be provided electronically if the customer requests or agrees to receive an electronic receipt.
- **Fraud warnings:** Specific to kiosk operators, kiosks must now make disclosures of "all material risks associated with virtual currency generally" before each transaction. HB1467 further specifies that those risks include (without limitation) the following: (1) lack of recoverability of funds, (2) virtual currencies are not subject to protections of the Federal

Deposit Insurance Corporation, National Credit Union Administration, or Securities Investor Protection Corporation, (3) volatility in virtual currency markets, and (4) the irreversibility of certain crypto transactions.

Additionally, before opening a customer's account, the kiosk operator needs to disclose (1) the customer's potential liability for unauthorized transactions, (2) any right for the customer to stop payment, (3) when a kiosk operator will disclose information about the customer to third parties, (4) the customer's right to get a receipt, (5) and any other customary disclosures.

Items Impacting Kiosk Functionality

In addition to the recission right, which will undoubtedly impact the required functionalities of kiosks, there are several other requirements impacting the ways that kiosk operators must design kiosks. Of note, though, many of these additional functionalities now required by Arkansas HB1467 have been commonplace among the industry. These requirements include:

- **Customer identification:** Kiosk operators must collect government-issued ID from each customer.
- **Wallet restrictions:** Kiosk operators must implement functionality that will prevent multiple customers from using the same virtual currency wallet.
- **Wallet blocking:** Kiosk operators must be able to block specific wallets from use at kiosks. Further, they must be able to identify and block high-risk or sanctioned wallets.
- **Post-transaction monitoring:** Kiosk operators must implement a risk-based method to monitor customer activity after transactions.

Staffing and Compliance Function Considerations

Arkansas HB1467introduces a few key provisions which may impact the personnel and training of kiosk operators. While the Bank Secrecy Act (BSA) imposes certain requirements on money

transmitters, HB1467 goes above this and prescribes certain requirements of compliance officers. This may impact the organizational structure within kiosk operators, particularly early-stage operators who are closely held and managed by a limited number of owners and managers. Consider the requirements below:

- **Chief compliance officer:** HB1467 introduces certain key requirements related to the CCO role within kiosk operators. First, CCOs must be qualified and responsible for ensuring legal compliance. Second, they cannot own more than 20% of the company.
- **Staffing:** Compliance duties must be handled by full-time employees.
- **Live support:** Kiosk operators must provide live phone support during kiosk operating hours, with the number clearly displayed.

Compliance and Data Security Programs

While money transmitters are required to comply with a number of requirements under the BSA, as well as other laws which states may adopt, HB1467adds additional requirements that are aimed at reducing elder financial abuse through the use of kiosks. These include:

- **Education and training requirements:** The law requires that licensees provide training materials (on an annual basis) to authorized delegates on elder financial abuse and how to respond when a delegate believes that they are being asked to engage in a transaction where an elder is suspected of being taken advantage of.
- **Elder adult safeguards**: Kiosk owners/operators must take the following steps to comply:
    - Speak with new elder customers before their first transaction.
    - Record the conversation, reconfirm attestations, discuss the transaction, and explain fraud risks.

- Approve transactions based on the outcome of this conversation.

Other Miscellaneous Considerations

Certain states proscribe rules regarding limitations on customers' use of the services of money transmitters. Recently, states, including Arkansas through HB1467, have significantly limited the ability for customers to freely interact with and use kiosk operator's services by implementing limitations on number and size of transactions in hopes that such limitations will prevent fraud and abuse. HB1467 sets forth other miscellaneous restrictions, while also providing a clear mechanism for consumers to make claims directly against the surety bond of money transmitters. Below are some provisions in this vein from HB1467:

- **Fee cap:** Operator fees are capped at $5 or 18% of the transaction.
- **Daily transaction limits:** Transactions are limited to $2,000 for new customers and $7,500 for existing customers, per day.
- **Surety bond:** The surety bond required for money transmitters must go to "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," while allowing consumer claimants to make direct claims against the bond.

Information Security Requirements

HB1467 classifies all "money services business licensed under [the Uniform Money Services Act]" as "financial institutions" within its Data Security for Money Services provisions, in addition to traditional money services businesses. As such, virtual currency kiosk owners and operators are required to meet the information security program requirements enacted within HB1467.

These requirements may pose significant challenges to virtual currency kiosk owners and operators depending on the size of their business. While traditional money services providers will likely have more experience in dealing with the regulatory frameworks imposed by laws such as Arkansas' Uniform Money Services Act, the inclusion of virtual currency kiosk owners and operators may be these businesses' first encounter with government-imposed information security regulations.

HB1467 requires that financial institutions (financial institutions, as noted above, are defined as any money services business licensed under Arkansas' Uniform Money Services Act) put in place a written information security program. Broadly, this program is required to contain administrative, technical, and physical safeguards 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 the financial institution holds. However, on a more technical level, financial institutions in Arkansas are now required by law to institute what were previously merely industry best practices. Although these requirements are absolutely in the interest of all financial institutions to achieve, doing so may present a challenge to mid-size financial institutions that only just meet the applicability threshold of the Data Security for Money Services provisions of HB1467 but that do not have the resources to fully implement a robust information security program.

Specific Information Security Program Requirements

After the passage of Arkansas HB1467, financial institutions are required to designate a qualified individual to lead their information security program and base their information security program on a risk assessment which: "(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) assess the sufficiency of any safeguards in place to control these risks."

The risk assessment must be documented in writing 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." Finally, financial institutions are now required to "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."

Once a risk assessment has been completed, financial institutions must design and implement safeguards to control the risks identified through their risk assessment. HB1467 gives a non-exhaustive list of controls that the financial institution is required to put in place. These safeguards include:

- Implementing and periodically reviewing access controls.
- Identifying and managing the resources which enable the financial institution to meet its business objectives.
- Encrypting all customer information in the financial institution's possession at rest and in transit, and to the extent that is infeasible, securing the customer information using effective alternative controls.
- Implementing a security program for applications used to transmit, access, or store customer information.
- Implementing multi-factor authentication for individuals accessing an information system.
- Developing data retention guidelines that include procedures for secure disposal of customer information 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:

- Necessary for business operations or for other legitimate business purposes;
- Otherwise required to be retained by state law or rule, or federal law or regulation; or
- Where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

- Reviewing the financial institution's data retention policy periodically.
- Adopting change management procedures.
- Implementing activity logging policies, procedures, and controls.

Financial institutions are also required to regularly test or otherwise monitor the effectiveness of their information security program and the requirements outlined above. Alternatively, they can conduct annual penetration tests and vulnerability assessments biannually and whenever there are material changes to the financial institution's operations or business arrangements and circumstances the financial institution knows or has reason to know may have a material impact on its information security program. Financial institutions are required adjust their information security program based on the steps taken above.

Arkansas HB1467 also requires that financial institution personnel be able to enact the information security policy by receiving security awareness training, utilizing qualified information security personnel, providing information security personnel with security updates and training, and verifying that key information security personnel maintain knowledge of changing information security threats and countermeasures.

HB1467additionally requires that financial institutions oversee their contractors by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards, require contractual terms with their contractors, and assess their contractors based on a risk analysis.

FBT Gibbons

Incident Response Plan

HB1467 requires that financial institutions establish an incident response plan designed to respond to, and recover from, security incidents which materially affect the confidentiality, integrity, or availability of the customer information in their control. The incident response plan must address:

- Goals of the plan;
- Internal processes for responding to an information security incident;
- Definition of roles, responsibilities, and decision-making authority;
- External and internal communications and information sharing;
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- Documentation and reporting regarding information security incidents and related incident response activities; and
- Evaluation and revision as necessary of the incident response plan.

Additional Requirements

- The individual who the financial institution appoints as its qualified individual must make at least annual reports to the financial institution's board or equivalent governing body.
- If no such body exists, the reporting obligations must be presented to a senior officer of the financial institution responsible for its information security program.
- HB1467 institutes regulatory notification requirements in certain instances of security incidents.
- The information security program requirements do not apply to financial institutions with less than 5,000 consumers' information.

FBT Gibbons

For more information or assistance navigating these new requirements under Arkansas HB1467, please contact the authors or any attorney with our Data, Digital Assets, and Technology or Consumer Financial Services and Protection practices.

FBT Gibbons