VERMONT

DEPARTMENT OF FINANCIAL REGULATION

Act No. 23 (2025) STUDY; BANKS; SUSPICIOUS ACTIVITY; TRANSACTION HOLD

January 15, 2026

Submitted by:
Kaj Samsom, Commissioner of Financial Regulation

Introduction

Section 17 of Act No. 23 of 2025, *An act relating to the regulation of insurance products and services*, requires the Department of Financial Regulation (DFR) to study regulatory models that would allow a financial institution to take measures to protect account holders from fraudulent transactions and to recommend a model for legislative consideration. The study shall include a review of regulatory models enacted or proposed in other jurisdictions.

DFR consulted with the organizations specified in the statute, including the Vermont Bankers Association, the Association of Vermont Credit Unions, AARP Vermont, the Office of the Attorney General, and Vermont Legal Aid. DFR also consulted with the Office of Adult Protective Services (APS) within the Agency of Human Services. Two virtual stakeholder meetings were held with the named entities, in June and in October.

Act No. 23 required DFR to provide a status report of preliminary findings and recommendations to the House Committee on Commerce and Economic Development and the Senate Committee on Finance no later than November 15, 2025, with a final report to be submitted no later than January 15, 2026. This report builds upon the November status report to provide a more complete discussion of DFR's background research and stakeholder conversations, in which consensus was reached on some but not all items.

DFR finds that suspicious transactions, including those caused by cyber fraud, are frequently encountered by financial institutions and by law enforcement, with many states enacting suspicious transaction hold laws. In response to the potential consumer losses associated with these transactions, DFR recommends the adoption of a statute providing banks and credit unions with the general discretion to voluntarily place a hold on a potentially suspicious transaction, along with appropriate liability protection. Additional details on the specifics to consider in such a statute are discussed below.

Background on Suspicious Transaction Holds

Banks and credit unions in Vermont routinely encounter situations where a customer is coerced into a potentially suspicious transaction as the result of scams or fraud. Once a customer has executed a transaction and subsequently recognizes that they have been defrauded, in most cases it is too late to regain lost funds. Many potentially suspicious transactions involve in-person activity, such as cash withdrawals or transfers, where frontline staff have the ability to intervene if given the tools to pause a transaction. DFR continues to explore how similar authority could effectively apply to online, mobile, and other types of remote transactions.

The ability to place a hold on suspicious transactions gives the customer time to reflect and step away from the urgency of a perpetrator's demands, and if necessary, gives the financial institution and other parties, such as law enforcement and APS, time to investigate. However, in some cases, transaction holds may also be viewed by customers as hostile acts, and in response, customers may close an account or attempt to execute a transaction by other means. As transactions become increasingly frictionless, particularly through nonbank payment apps, the ability to pause a

suspicious transaction is both challenging to implement universally and critical to protect consumers from fraud.

The FBI's most recent Internet Crime Complaint Report (IC3 Report) notes that nearly 860,000 complaints were received in 2024 about cyber fraud nationwide, resulting in $16.6 billion in losses.[1] Vermonters filed 937 complaints about cyber fraud to the FBI (44th in the country on a per-capita basis), with $11.3 million in reported losses (49th on a per-capita basis). 243 complaints from Vermonters were filed by people age 60 or older, with $4.2 million in losses.[2] These losses were due to a wide range of fraudulent activity, including romance scams, employment scams, extortion, government impersonation, investment scams, lottery and sweepstakes scams, tech support scams, and threats of violence. Cryptocurrency transactions and wire or ACH transfers were identified as the two most common ways in which people lost money in fraud situations.[3] Even fraudulent activities that eventually take place electronically, such as a cryptocurrency transaction or prepaid card purchase, may begin with a cash withdrawal at a bank or credit union.

Since many victims may choose not to file a report with law enforcement, the actual incidence and losses may be even higher than these numbers would suggest. One recent analysis estimated that 7 in 10 victims reported scams to their financial institution, while only 1 in 10 reported to local law enforcement and 1 in 17 reported to a federal agency.[4] This highlights financial institutions' trusted position in the community and the important role they play in preventing fraudulent activity. After accounting for under-reporting, annual fraud-related consumer losses could be nearly ten times higher than known estimates.

DFR has identified at least 26 states that currently have a suspicious transaction hold law, also known as a "report and hold" law; an appendix lists these states along with citations to each state's law.[5] While these primarily apply to banks and credit unions, precedent also exists for other types of financial products. For example, FINRA Rule 2165 provides a safe harbor for broker-dealers to place temporary holds on securities transactions and disbursements in cases of potential financial exploitation.[6] Vermont has also adopted through regulation the NASAA Senior Model Act which requires that qualified individuals including broker-dealers and investment advisors report and hold suspicious securities transactions.[7]

---

[1] Federal Bureau of Investigation, "Internet Crime Report 2024," April 2025, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[2] Since reporting age is optional, it is possible that additional older Vermonters were among total complaints filed.
[3] Other payment methods noted as potentially leading to fraud, in declining frequency, were card payments, peer-to-peer transfers, gift or prepaid card transactions, checks, and cash.
[4] The Aspen Institute, "United We Stand: A National Strategy to Prevent Scams," September 2025, https://fraudtaskforce.aspeninstitute.org/nationalstrategy.
[5] 24 of these state laws were listed in an October 2024 FTC report. https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/FinancialInstitutionTransactionHoldsStateOverview.pdf
[6] FINRA, "Frequently Asked Questions Regarding FINRA Rules Relating to Financial Exploitation of Senior Investors," https://www.finra.org/rules-guidance/guidance/faqs/frequently-asked-questions-regarding-finra-rules-relating-financial-exploitation-seniors
[7] V.S.R. § 8-4, Protection of Vulnerable Adults from Financial Exploitation.

Based on research and stakeholder conversations, DFR recommends that the General Assembly adopt a statute that provides banks and credit unions with the general discretion to voluntarily place a hold on a potentially suspicious transaction, along with appropriate liability protection. The criteria for placing such a hold should be consistent with statutes in other jurisdictions that have acted in this area, and should be flexible, based on the nature of the individual's behavior and the nature of the transaction. While general patterns of behavior may suggest potentially suspicious activity, scam and fraud practices change regularly. An overly prescriptive approach may not be able to keep up with emerging threats.

Discussion of Specific Topics in Section 17

Based on research and stakeholder conversations, DFR offers the following discussion and, where applicable, recommendations for the specific items (#1-8) mentioned in Section 17 of Act 23. In general, DFR aimed to reach stakeholder consensus on these items, and consensus was reached for many of them. However, there were dissenting views in some areas that merit additional consideration and discussion.

1. Financial institutions subject to the proposed model

Most states' transaction hold laws apply to depository institutions, such as banks and credit unions, whether they are chartered in that state or not. Michigan and Nebraska apply their suspicious transaction hold laws to institutions covered by deposit insurance that operate in that state. Some states, such as Alabama, Arkansas, Minnesota, Tennessee, and Virginia, include various types of nonbank lenders as well. Some states also explicitly include or exclude broker-dealers and investment advisers; these may also have their own authorities under other laws. Tennessee's law also extends to check cashers, and Virginia's includes insurance companies.

A suspicious transaction hold law should apply to all banks and credit unions operating in Vermont, including Vermont-chartered, out-of-state, and national institutions. DFR continues to explore whether other types of financial institutions should be subject to similar requirements to the extent they are not already.

2. Whether specific account holders should receive heightened protection

A suspicious transaction hold policy should not single out any particular population. Fraud and scams can occur to any customer at any age. Some types of scams, including cryptocurrency, investment, and romance scams, may frequently target younger consumers as well as older ones. In the FBI's IC3 report, among complaints where the complainant provided their age, the majority of complaints in some scam categories—including employment, investment, and non-delivery of goods scams—were made by those under 50 years old.

Instead of focusing on specific account holders, financial institution policies should focus on the specific aspects of the customer's behavior and the suspicious transaction to make a determination about whether to place a hold. If employees were to focus solely

on specific types of account holders, holds could ultimately be arbitrary or biased, while other suspicious transactions continued without being identified.

At the same time, there are populations already recognized in Vermont's APS statutes that are particularly vulnerable, including people with disabilities; people who are unable to protect themselves from abuse, neglect, or exploitation; residents of facilities; and people receiving long-term personal care services.[8]

DFR recommends that suspicious transaction holds apply to any customer or transaction meeting the institution's discretionary criteria, regardless of age or other status. Institutions must also comply with existing APS statutes to ensure vulnerable adults are protected.

3. Notification and consultation requirements

Accounts where multiple parties have access present difficult scenarios for suspicious transaction holds. While helpful in some circumstances, notifications in other situations could be a violation of privacy or even contribute to harm. In some cases, the other party with access to the account may be the individual engaged in financial exploitation. Stakeholders noted the potential abuse of powers of attorney (POA) when an agent empowered under a POA makes decisions that are not in the principal's best interest. The adequacy of POA requirements is outside DFR's scope and is a subject for further exploration.

Some have pointed to the use of a trusted contact—an individual who does not have access or control over the account, but could be contacted in case of a potentially suspicious transaction. A customer could be asked in a low-stress environment, such as the time of account opening or at another convenient time, if they would like to name another person whose information would be on file if case of a problem with their account. If an employee later believes that a particular transaction is suspicious, notifying the trusted contact would alert that person to a potential concern, and they would then be encouraged to get in touch with the customer to assess the situation. For example, a relative or neighbor might be able to speak with the customer and verify if the transaction is legitimate, or dissuade them from executing that transaction.

In some circumstances, a trusted contact would be highly effective as a prevention tool, but its value is not universal and in some cases may be detrimental. The trusted contact on file must remain current, yet a change in one's trusted contact may also raise red flags. It may be difficult to determine if a new trusted contact is legitimate, or is coercive or fraudulent. There may also be circumstances in which a trusted contact could stand to benefit from a suspicious transaction, which defeats the purpose. In other situations, the transaction may be legitimate, but the customer would prefer that it remain private.

DFR does not recommend imposing any new requirements for notification or consultation with third parties connected to an account, such as joint account holders, fiduciaries, or trusted contacts. DFR supports banks and credit unions offering the

[8] A full definition of "vulnerable adult" is contained in 33 VSA § 6902(34).

option to add a trusted contact—an individual the customer knows, but who does not have access or control over the account—recognizing that it is a complex individual decision. In general, a trusted contact should be identified by a customer in the ordinary course of business, at a non-stressful moment for the accountholder. In case of a suspicious transaction, the bank or credit union may then notify the trusted contact about the transaction. However, the bank or credit union should not notify the trusted contact if the trusted contact is suspected of participating in financial abuse. If the customer does provide a trusted contact, the institution should annually revisit whether the trusted contact is up to date.

4. Reasonable time periods for transaction holds

Most state transaction hold laws specify the length of time for an initial hold and an extended hold, although some provide for a general hold until the financial institution does not expect the transaction to result in financial exploitation. Most initial holds range from a few days up to 15 business days, with extended holds continuing beyond one month (in some cases as long as 45 business days). In many states, holds can generally also be extended under a court order or if an investigation is ongoing by a bank or credit union, by law enforcement, or by Adult Protective Services.

Stakeholders identified two key principles in favor of longer time periods. Some noted that the longer a transaction hold is in place, the more likely it is that the customer, potential trusted contact, or someone else close to them will recognize the transaction as suspicious, making it more likely that they withdraw that transaction voluntarily. Additionally, longer time periods enable third parties to do their work. For situations involving a vulnerable adult, it may take up to ten days for APS to conduct its assessment after being notified. If a customer is under APS review, a potentially suspicious transaction should not be able to go forward until its assessment is complete.

DFR does not recommend a specific hold length, but suggests that a reasonable transaction hold should last a minimum of 15 days, to be extended up to 30 days upon request by law enforcement or APS. There may also be circumstances in which a 30-day hold is insufficient to complete an investigation, which may warrant an extended hold. For cases under referral to APS, the hold should be sufficiently long enough to complete an assessment.

5. Notification to DFR, law enforcement, and other third parties

Notification to public agencies can serve two purposes: problem resolution for the victim, and market monitoring for the incidence of suspicious transactions. Suspicious transactions may already be reported to federal law enforcement in the form of a Suspicious Activity Report (SAR); however, these reports are confidential and their utility may vary. DFR recommends notification of specific suspicious transaction holds to local law enforcement, with referral to APS when appropriate in the case of a vulnerable adult. This provides for additional supports to the customer when possible.

Anonymous information about suspicious transaction holds is also valuable to policymakers and financial institutions. Based on this information, they may be able to identify trends or patterns that help determine where to deploy resources, including customer education and employee training. This information may also help prevent repeat offenses by perpetrators of fraud and scams. In some cases, financial institutions, law enforcement, and other entities already share some of this information to raise awareness of emerging trends and best practices.

To that end, DFR also recommends anonymous reporting from financial institutions about the frequency of transaction holds to appropriate state authorities. This reporting would not include any personal information, but could include demographic information such as age or location. Anonymous reporting should only be used for monitoring and tracking purposes, and should not be burdensome on the financial institution. To the extent possible, summaries of anonymous reporting should be made available to financial institutions, policymakers, and the public.

6. Continued account holder access to funds

Stakeholders generally agreed that in the event of a potentially suspicious transaction, account holders should continue to have access to all of the other funds in their account. The presence of a suspicious transaction should not impede their ability to pay their rent, mortgage, or other bills, or to receive incoming deposits. Particularly if a transaction hold is in place for an extended period (as discussed in #4 above), maintaining access to other funds is crucial. However, it is possible that by not protecting other funds, an individual may attempt to participate in other suspicious transactions by other means.

DFR recommends that a suspicious transaction hold only apply to suspicious transactions, and not to the remaining balance in an individual's account or any other accounts at that institution. A question was raised in stakeholder conversations about whether other mechanisms are also necessary to protect accountholders, such as limitations on online account access or activity; this is an issue for further exploration.

7. Immunity from civil liability

In general, immunity from civil liability at a minimum provides a safe harbor for employees and financial institutions to identify suspicious transactions without concerns of retaliation. However, in some circumstances, limiting immunity may be warranted. For example, in the event of a potentially suspicious transaction that is held for an extended period of time, but is in fact a legitimate transaction, it may be appropriate for a customer to seek redress.

Other states' laws on suspicious transaction holds vary in terms of relief from civil, criminal, or administrative liability. Some state laws apply immunity to financial institutions and employees acting in good faith, which may be a subjective determination. Others consider financial institutions and employees to be generally immune unless grossly negligent. Louisiana's statute does not extend immunity to individuals who were involved in financial exploitation, or in cases of gross negligence

resulting in losses to the victim of financial exploitation. South Carolina's statute maintains civil liability against a financial institution for participating in or materially aiding the financial exploitation of a vulnerable adult.

DFR recommends that financial institutions and employees placing suspicious transaction holds receive some form of civil immunity, which will encourage voluntary reporting. However, DFR defers to the General Assembly to determine the particular categories and levels of immunity, and any applicable exemptions. (For example, in some states, financial institutions and their employees are immune from criminal, civil, and administrative liability.) Immunity provisions should not conflict with DFR's existing direct enforcement authority over chartered institutions.

8. Other provisions

Notably, some states impose training requirements on financial institution employees. These include one-time or periodic (e.g. annual) requirements to complete training. Training helps individuals to recognize fraudulent activity and financial exploitation, to be aware of current scams and fraud, and to know the options for placing transaction holds and taking other steps to prevent additional harm. Some financial institutions may also already conduct training in the absence of a specific statutory requirement.

Many sources of training already exist, including AARP's BankSafe, the federal Financial Crimes Enforcement Network (FinCEN), American Bankers Association, Independent Community Bankers Association, and others. Adult Protective Services offers a virtual "APS 101" training for financial institution employees which covers reporting requirements and expectations. In addition to financial institution employees, training may also be valuable for other parties who interact with vulnerable adults, including law enforcement, senior centers, Area Agencies on Aging, home health agencies, and others.

DFR recommends periodic training requirements for financial institution employees to recognize potentially suspicious transactions and their authorities to resolve them. DFR also recommends continued outreach and coordination between banks, credit unions, and organizations outside of the financial industry so that they may better identify, prevent, and resolve suspicious activity.

Conclusion

Through suspicious transaction holds, banks and credit unions have the ability to prevent fraudulent activity on customers' accounts and safeguard their funds. Other states' statutes provide a reasonable framework for enacting similar protections against fraud and scams in Vermont.

Appendix: States with Suspicious Transaction Hold Laws

Alabama (Ala. Code 8-6-190 et seq.)
Arkansas (AR Code Ann. 4-88-208)
Connecticut (CGS 26a-253)
Delaware (Del. Code Ann. 31, Section 3901 et seq.)
Florida (F.S. 415.10341)
Idaho (Id. Code 27-67-2763)
Kentucky (Ky. Rev. Stat. Ann. Section 365.245)
Louisiana (La. Rev. Stat. Ann. Section 6:1371 et seq.)
Maine (9-B MRSA 245)
Michigan (Mich. Comp. Laws Section 487.2081 et seq.)
Minnesota (Minn. Stat. Section 45A.06)
Mississippi (Miss. Code Ann. Section 81-5-107)
Montana (Mont. Code Ann. Section 32-1-1501)
Nebraska (Neb. Rev. Stat. Section 8-2903)
Nevada (slightly different cite from above: 657.220 et seq.)
New Hampshire (N.H. Rev. Stat. Section 383-A:5-511-a)
North Dakota (N.D. Cent. Code Section 6-08.5-01 et seq.)
Oregon (Or. Rev. Stat. Ann. Section 708A.670 et seq.)
Rhode Island (R.I. Gen. Laws Section 19-34-1 et seq.)
South Carolina (S.C. Code Section 43-35-87)
Tennessee (Tenn. Code Ann. Section 45-2-1201 et seq.)
Texas (Tex. Fin. Code Section 281.001 et seq.)
Utah (U.C.A. 1953 Section 7-26-101 et seq.)
Virginia (Va. Code Ann. Section 63.2-1606)
Washington (Wash. Rev. Code Section 74.34.215 et seq.)
Wyoming (Wyo. Stat. Ann. Section 13-1-701 et seq.)