Montana Blockchain and Digital Innovation Task Force

Meeting Minutes

Date: June 1, 2026
Time: 9:00 a.m. - 12:34 p.m.
Location: Montana State Capitol, Room 455 (hybrid meeting with in-person and virtual attendance via Zoom)
Website: https://doa.mt.gov/bfid/bditf

Call to Order and Recording Notice

Representative Curtis Schomer the meeting of the Blockchain and Digital Innovation Task Force to order and stated that he was co-chairing with Senator Daniel Zolnikov. Co-chair Schomer also announced that the meeting was being audio and video recorded.

Roll Call

Legislators Present

- Representative Curtis Schomer
- Representative Kelly Kortum
- Senator Shane Morigeau
- Senator Daniel Zolnikov

State Officials and/or Designees Present

- Commissioner James Brown
- Kirsten Madsen, Deputy Securities Commissioner, Representative for Commissioner James Brown
- Trevor Graff, Director of Government Affairs, Representative for Commissioner James Brown
- Alan Doane, designee for Attorney General Austin Knudsen

Industry & Public Members Present

- Mark Baker
- Loren Brown
- Randy Chesler
- Leigh Drogen
- Julie Fredrickson
- Alex Miller
- Daniel Pittman
- Sam Sill

Members Excused or Not Present as Called

- Senator Gayle Lammers
- Representative Ler

- Tanner Avery
- Bill Bickle
- Kevin Gilbertson
- Guillermo Perez
- Thad Pryor

Approval of Prior Minutes

Representative Schomer moved to approval of the April 23, 2026, meeting minutes. Sam Sill made the motion to approve, Loren Brown seconded, no objections were raised, and the motion passed.

Presentation: Division Of Banking and Financial Institutions — Stablecoins and the GENIUS Act

Presenter: Melanie G. Hall, Commissioner, Department of Administration, Division of Banking and Financial Institutions

Commissioner Hall opened with a disclaimer that the Division's presentation is not a statement of official Department of Administration policy, governor's office policy, or legal advice.

Objectives of the Presentation

1. Provide an update on state stablecoin legislation and GENIUS Act-aligned state pathways.
2. Compare other states' Permitted Payment Stablecoin Issuer (PPSI) pathways.
3. Discuss Task Force recommendations.

GENIUS Act Overview

The GENIUS Act (Guiding and Establishing National Innovation for US Stablecoins Act) was passed into law on July 18, 2025. It creates a national regulatory framework specifically for payment stablecoins and their issuers. Key points:

- Limits the issuance and sale of payment stablecoins in the U.S. to Permitted Payment Stablecoin Issuers (PPSIs).
- PPSIs must maintain specific reserve assets, meet capital standards, and comply with all Bank Secrecy Act (BSA) and anti-money laundering (AML) laws.
- The Act offers both a federal licensing path (through the Office of the Comptroller of the Currency, OCC) and an optional state licensing path.
- This is not applicable to Bitcoin or other investment-type cryptocurrencies — it applies only to stablecoins pegged to the U.S. dollar.

GENIUS Act Key Implementation Dates

Date	Milestone
July 18, 2025	GENIUS Act signed into law.

Date	Milestone
January 18, 2027	GENIUS Act takes effect (earliest of 18 months after enactment, or 120 days after federal regulators issue final rules).
January 18, 2028	State initial certification deadline (1 year after effective date). Potential extension exists for states that miss the deadline.
July 18, 2028	Deadline for sale of non-PPSI stablecoins in the U.S. After this date, anything called or issued as a stablecoin must be issued by a PPSI.

State pathways must be "substantially similar" to the OCC's framework — states cannot set lower capital thresholds, compliance standards, or otherwise easier requirements than the federal pathway.

State Stablecoin Legislation — Current Landscape (as of May 24, 2026)

Status	State / Bill	Notes
Pending	North Carolina — HB 1029	Digital Asset & Stablecoin Act (introduced April 21, 2026; assigned to House committee)
Pending	Delaware — SB 19/SS 2	Passed Senate; assigned to House committee
Enacted	Alabama — HB 259	Enacted April 6, 2026; effective October 1, 2026
Enacted	Georgia — HB 1272	Enacted May 11, 2026; effective earlier of January 18, 2027, or 120 days after federal rules are finalized
Enacted	Maryland — SB 662	Enacted May 12, 2026; effective January 1, 2027
Enacted	Minnesota — HF 3709	Crypto custody bill, no PPSI framework; enacted May 15, 2026; effective August 1, 2026

Commissioner Hall noted that states with money transmitter licensing frameworks have a stronger regulatory interest in this space, as money transmitters are expected to be significant PPSI applicants. Montana does not currently license money transmitters, which creates a different calculus — Montana would not lose regulatory revenue by not acting, unlike most other states.

Policy Considerations for Montana

Commissioner Hall outlined four key questions the Task Force should consider:

1. Who is the primary regulator? (Banking vs. Securities and Insurance — both offices indicated a preference to defer.)
2. Is there an explicit commitment to "substantial similarity" with OCC standards?
3. What is the best balance for state rulemaking authority? (More flexible rulemaking allows agencies to respond to changes; more restrictive statutory language is challenging in Montana given biennial sessions.)
4. How best to maintain core GENIUS measures regarding capital, assets, and AML compliance?

Policy Choices and State Examples

Policy Choice	High-Level Option	State Examples
Regulatory structure	Separate issuer (GENIUS) and service-institution (state) tracks	Maryland
Federal vs. state emphasis	More federal-centric compliance model	Alabama
State oversight role	Stronger ongoing state regulator role	Delaware, North Carolina
Statutory design	More heavily codified in statute	Delaware, Georgia
Prudential detail	Very detailed requirements	Delaware, Georgia
Market-access timing	Explicit future ban on non-permitted issuers post-7/18/2028	Alabama, Georgia
Rulemaking approach	GENIUS-aligned guardrails with more regulator-led implementation	Delaware, North Carolina
Growth/transition trigger	$10B threshold with specified transition processes	Delaware, North Carolina
Crypto custody and services	Allow state banks and credit unions to offer crypto custody services (does not create GENIUS PPSI framework)	North Carolina, Minnesota

Task Force Recommendation Options Presented

1. Proceed with a Montana state-qualified stablecoin issuer bill.
2. Wait for finalized federal GENIUS Act rules (expected by end of summer 2026), then decide.
3. Rely solely on the OCC federal pathway, allowing Montana businesses to become PPSIs under federal law without a state framework.

Discussion

Senator Zolnikov: Asked Commissioner Hall whether she was now among the most advanced state banking commissioners in the country given the pace of her engagement with these issues.

Commissioner Hall: Noted that some states like Georgia have moved more quickly, in part because they regulate money transmitters and have a financial stake in the outcome. She noted she is the fifth-longest-serving banking commissioner in the country at 15 years. Senator Zolnikov suggested the Task Force simply take no action on this issue at this time, directing that this position be included in the report.

Leigh Drogen: Concurred, stating most PPSI companies would prefer nationally licensed, and it makes more sense to wait for national regulatory parameters before adding a state layer. He also expressed a preference for larger, nationally licensed players to lead adoption in the short term to build confidence in the system.

Alex Miller: Agreed, emphasizing the importance of not impeding innovation. He noted Montana's unique status as a non-money-transmitter-licensing state may already provide fewer barriers for innovation, making a state framework less urgent.

Sam Sill: Stated that with federal rulemaking ongoing, anyone interested in these policy areas will be making decisions in the summer regarding the next legislative session. He recommended waiting to see what the rulemaking says before reinventing the wheel at the state level.

Commissioner Hall: Noted that if states could create simplified frameworks with lower capital thresholds, there would be a stronger case for state action. However, since state pathways must be substantially similar to the OCC's standards, the benefit of a state framework is limited.

Co-Chair Schomer: Expressed personal support for allowing the federal process to run its course, noting his concern about legislation that could hinder small businesses or innovation.

Senator Zolnikov: Made a motion that the Task Force take no action on the stablecoin issuer bill issue, with this position noted in the report. He also suggested the possibility of granting the banking agency general rulemaking authority as a flexible option, while acknowledging the risk that future commissioners could use such authority to enact stringent regulations.

Co-Chair Schomer: Agreed the consensus was to let the federal process proceed.

Consensus

The Task Force agreed to recommend taking no action on a Montana state-qualified stablecoin issuer bill at this time, and to rely on the OCC federal pathway. This position will be included in the Task Force's report to the Economic Affairs Interim Committee (EAIC).

Presentation: Montana Grain Growers Association — Blockchain and Agricultural Technology

Presenter: Steve Sheffels, President, Montana Grain Growers Association (via Zoom)

Commissioner Hall introduced Steve Sheffels, who joined remotely. Mr. Sheffels farms northeast of Great Falls, growing wheat, barley, peas, and winter canola. The Montana Grain Growers Association represents approximately 5 million acres in production, with about 700 producer members and 250 associate members, primarily from the Golden Triangle and northeastern Montana.

Blockchain in Agriculture

Mr. Sheffels stated that blockchain has been discussed only lightly within the organization. The most prominent potential application he identified is two-way traceability in the supply chain — as demonstrated by recent food recalls involving lettuce and meat, where blockchain helped identify the source of contamination. However, he expressed significant skepticism about its practical application to bulk grain handling, citing several structural barriers:

- Grain from across an entire farm is commingled in large bins (the largest holding one-third of the farm's crop), eliminating field-level traceability.
- Grain sold to local mills (such as Grain Craft in Great Falls) is mixed with grain from other producers on delivery.
- The bulk handling system, including grain bins emptied from the bottom, makes physical separation impractical without dedicated, separate storage.
- The mechanical nature of bulk grain handling makes it difficult to maintain hard lines between product sources.

He noted one example where separation does occur: GMO versus non-GMO canola, where the local crush plant in Great Falls requires non-GMO canola only, creating a traceable stream by plant source. He also noted that the local malt plant traces grain by truckload and tracks movement from elevator to malt house, suggesting limited traceability is already occurring in some segments of the supply chain.

Discussion

Co-Chair Schomer: Asked whether blockchain technology had been discussed, and whether the Grain Growers would be interested in it.

Mr. Sheffels: Acknowledged both the potential upside (achieving a premium for Montana's high-quality growing environment) and the fears (liability concerns if a farm were incorrectly identified as the source of a health event in a blockchain trace).

Commissioner Hall: Asked about other digital and AI technologies being adopted in agriculture, and whether the Montana Department of Agriculture was collaborating on blockchain education.

Mr. Sheffels: Described several relevant technologies currently in use or emerging:

- GPS guidance on tractors is now universal, reducing overlap in seeding and spraying and cutting input costs.
- A precision sprayer system ("WeedIt") uses infrared/LED technology to identify and spray only green weeds rather than broadcasting herbicide — reducing herbicide use by approximately 80% in certain passes (from 5 gallons per acre to 1 gallon per acre in the final summer fallow pass).
- AI-driven predictive fertilizer application using soil sample datasets is beginning to emerge.
- The next technological frontier is crop/weed differentiation in fully green fields — distinguishing crop plants from weeds within the same field using camera-based AI systems. This is already showing success in corn country.

Mr. Sheffels confirmed a close relationship with the Montana Department of Agriculture but noted no current blockchain-specific programs. He noted that the Department is considering an AI-based grain scanner to increase throughput at the state grain lab in Great Falls.

Senator Zolnikov: Noted that while a farmer's concern about spotlight and liability is understandable, the benefit of blockchain traceability — narrowing a recall to specific stores rather than pulling product across 18 states — could dramatically reduce economic harm and consumer costs.

Mark Baker: Asked whether the Montana Department of Agriculture was collaborating with the grain growers on blockchain education similar to programs the Colorado Department of Agriculture has offered, including a webinar series on how the grain industry utilizes blockchain technology for supply chain data sharing.

Mr. Sheffels: Was not aware of current Montana programs but confirmed ongoing close communication with the state agency.
Co-Chair Schomer thanked Mr. Sheffels and closed the discussion.

Break

The meeting recessed briefly to allow for AV personnel transition and to admit additional virtual presenters.

Presentation: Coinflip — Cryptocurrency Kiosk Operations and Consumer Protection

Presenter: Jon Turke, Director of Government Affairs, CoinFlip (via Zoom)

CoinFlip Overview

Mr. Turke presented on behalf of CoinFlip, a digital assets platform based in Chicago that facilitates the purchase and sale of select cryptocurrencies via kiosk. CoinFlip operates in nearly every state, Washington D.C., and Puerto Rico, as well as internationally (Canada, Australia, New Zealand, Spain, Italy, and South Africa). CoinFlip holds 41 money transmitter licenses across the country, applying even in jurisdictions where not required. CoinFlip has over 4,000 kiosk locations in the U.S.

Leadership and Compliance Team

- Colleen Kavanaugh, Chief Legal Officer — former Assistant U.S. Attorney, Northern Districts of California, and New York
- Larry Lipka, General Counsel — formerly Illinois Attorney General's office
- Todd McElduff, Interim Chief Compliance Officer — former global financial crimes positions at PayPal and Morgan Stanley
- Jed Ruppers, Director of Law Enforcement Relations — former senior special agent, Wisconsin Department of Justice Cyber Crimes Unit, specializing in crypto crimes

Kiosk Operation and Transaction Process

Mr. Turke described CoinFlip kiosks as accessible points for consumers to purchase cryptocurrency using cash at convenience stores, gas stations, and grocery stores. The company pays host businesses several hundred dollars per month in rental fees for kiosk placement. He walked through the transaction process:

1. Every customer first sees the "Safe in Six" screen — a consumer protection framework designed to help users spot a scam before transacting. Users must acknowledge six key points, including that all transactions are final and irreversible, that they fully own and control the wallet being used, and that they agree to the privacy policy and terms of service.
2. Users then receive and enter a one-time SMS passcode (phone number verification).
3. New customers complete a simple registration providing full name, date of birth, and phone number.
4. For transactions over $1,000, customers must complete additional verification: scanning a QR code, taking a selfie, and uploading a government-issued ID. This usually takes one to two minutes.
5. For transactions over a specified threshold (generally just under $3,000), customers must provide their Social Security number, occupation, purpose of transaction, and source of funds.
6. The fee percentage and total transaction amount are clearly displayed before the transaction is finalized; receipts are sent via SMS and email.
7. Cryptocurrency settlement may be delayed at CoinFlip's discretion to provide additional fraud protection, which is particularly beneficial for new customers.

Consumer Protection Measures

- 24/7/365 live customer support staffed by CoinFlip employees (not contractors), trained twice yearly in AML and scam indicators.
- "Safe in Six" fraud awareness campaign on kiosk screens.
- Tiered KYC requirements for larger transactions.
- Enhanced screening for customers who are 80 and older: customers in this age group must speak with a trained specialist before transacting.
- Wallet screening to block sanctioned or high-risk wallets.
- Wallet pinning: each wallet is linked to a specific user, preventing wallet sharing.
- Transaction holds for geographic anomalies (e.g., account registered in Wisconsin, transaction attempted in Minnesota — photo comparison required).
- Live transaction monitoring by compliance team.
- Blockchain analytics tools (Elliptic, TRM Labs, Chainalysis) to flag high-risk wallets and transaction patterns. TRM Labs reported approximately 1.2% of total kiosk activity was scam-related — described as comparable to traditional finance.

Legislative Engagement

CoinFlip has lobbied in 46 states and at the federal level through the 2026 legislative sessions. Approximately 27 states have enacted kiosk-related laws to date, with more than 30 expected by year-end. CoinFlip advocates for 72-hour settlement holds for new customers, noting that most victims realize they have been scammed within 24 to 48 hours.

Refund Policy

CoinFlip operates a refund process accessible via their website. They always refund transaction fees to confirmed fraud victims. Some states require full refunds for new customers within a specified period

(e.g., Minnesota requires refunds for new customer transactions reported as scams within 72 hours, with approximately 1% of Minnesota transactions resulting in refund requests). Principal recovery is complicated by the fact that CoinFlip sells cryptocurrency from its own inventory — a refund means CoinFlip is out both the cryptocurrency and the cash.

Mr. Turke noted that CoinFlip described itself as "the only financial services product in the entire country that refunds scam activity." Refunds are issued by check or electronic funds transfer; in some cases, customers have requested Bitcoin refunds.

Discussion

Co-Chair Schomer: Asked about the frequency and nature of refunds.

Mr. Turke: Confirmed the process as described above and reiterated that principal on confirmed scam transactions is refunded in states with such requirements.

Commissioner Hall: Asked what percentage of completed CoinFlip transactions turn out to be fraud or scams.

Mr. Turke: Stated approximately 1%, based on a combination of consumer reporting and blockchain analytics monitoring. He noted that Minnesota, which has had a refund law in place the longest (since 2024), showed approximately 1% of transactions requesting refunds.

Tom Pallach (member of the public): Asked how refunds are returned to the customer and was advised that refunds are issued by check or electronic transfer, not through the kiosk.

Break

Co-Chair Schomer called a brief recess.

Presentation: AARP — Cryptocurrency Kiosk Fraud Prevention

Presenter: Clark Flynt-Barr, Government Affairs Director for Financial Security, AARP (via Zoom)

Ms. Flynt-Barr introduced herself, noting her background as a former intelligence analyst with the FBI focused on crypto-enabled crime and prior work at Chainalysis, a blockchain analytics company. AARP represents the interests of Americans over 50, with a particular focus on financial fraud affecting older adults who have accumulated retirement accounts, brokerage accounts, and home equity.

The Problem — Cryptocurrency Kiosk Fraud

Ms. Flynt-Barr described cryptocurrency kiosks (also known as crypto ATMs, BTMs, or virtual currency kiosks) as machines found in grocery stores, convenience stores, malls, and restaurants that convert cash into cryptocurrency. These machines have become a primary vehicle for financial fraud targeting older adults.

Ms. Flynt-Barr played a CNN video illustrating how victims across multiple states were directed to deposit thousands of dollars into crypto kiosk machines by scammers impersonating banks, government agencies, and others.

Montana-Specific Kiosk Data

- The marketing website CoinATM Radar lists 31 kiosks in Montana, but the Commissioner of Securities and Insurance (CSI) estimates there are approximately 400 cryptocurrency kiosk machines operating in the state.
- Montana had 69 FBI IC3-reported complaints involving cryptocurrency kiosks in 2025, totaling $1,585,079 in losses — acknowledged as a significant undercount given the estimated 10–15% reporting rate.

National FBI Data (2025)

- 181,565 total cryptocurrency fraud complaints — a 21% increase from 2024.
- $11.366 billion in total losses — a 22% increase from 2024.
- 18,589 complainants lost more than $100,000; average loss of $62,604.
- More than half of all 2025 fraud and scam losses moved in cryptocurrency, even though crypto complaints represent only approximately one-fifth of total fraud reports.
- Adults 60+ suffered $4,432,224,488 in cryptocurrency fraud losses.

Crypto Kiosk-Specific National Data (2025)

- 13,460 complaints; $389 million in losses.
- 23% increase in complaints from 2024; 58% increase in losses from 2024.
- Adults 60+ experienced $257,466,130 (approximately 76%) of all age-reported crypto kiosk losses.
- Criminals stole an average of $41,607 from older victims in crypto kiosk-related fraud.
- The community economic impact extends beyond individual victims: losses represent approximately 1.8 years of housing expenses, nearly 5 years of healthcare expenses, 4.4 years of discretionary travel spending, 8 years of local grocery sales, and 9 years of local government utility revenue lost.

Iowa Attorney General Investigation

An Iowa AG investigation into Bitcoin Depot and CoinFlip found that 98.16% of money sent through Bitcoin Depot and 94.92% of money sent through CoinFlip were scam transactions, based on calling the top 20 customers of each company and finding all identified as fraud victims. Iowans lost more than $20,426,616 in these transactions.

State Legislative Landscape

- In 2023, only California and Connecticut had enacted crypto kiosk laws.
- By 2026, 30 states have enacted cryptocurrency kiosk laws; two additional bills are pending gubernatorial signature, which will bring the total to 32.
- Three states — Indiana, Minnesota, and Tennessee — have enacted full bans on cryptocurrency kiosks.

- Cities/municipalities with full bans include Spokane, Anacortes, and Kennewick (Washington); Heber City and Layton City (Utah).

Why Minnesota Moved to a Ban

Minnesota passed a law in 2024 with transaction limits for new users (first 48 hours) and other provisions. However, law enforcement found the law was not stopping fraud — scammers continued sending seniors to machines, reused email addresses and wallet numbers, gamed new-customer rules, and waited out the 48-hour period before continuing to victimize the same person. Indiana and Tennessee similarly began with regulatory bills but moved to full bans after further review.

Federal Legislative Activity

- S. 710, Crypto ATM Fraud Prevention Act of 2025 — introduced February 2025; largely tracks state-level provisions but has not gained significant traction.
- H.R. 3633, Digital Asset Market Clarity Act of 2025 (the "Clarity Act") — broader cryptocurrency market structure legislation. The Senate Banking Committee advanced it in a bipartisan 15-9 vote on May 14, 2026. Importantly, initial language would have preempted all state kiosk laws; after AARP and state regulators educated lawmakers, state preemption language was removed from the final markup. No state preemption currently in the bill.
- Despite federal activity, passage of comprehensive federal kiosk law is unlikely in the near term given remaining steps and the approaching midterm period.

Ms. Flynt-Barr urged Montana to move forward with its own state legislation, stating that federal protection is years away and Montanans need protection now.

Policy Provisions AARP Recommends for Montana

1. Daily transaction limits — AARP recommends a single $1,000 daily limit for all users (not tiered or increasing for repeat users). Industry median transactions are approximately $350. Tiered limits have proven ineffective because scams often unfold over weeks, with scammers starting small and escalating.
2. Refund requirements — Operators should be required to refund fraud victims; this creates a financial incentive for genuine compliance investment.
3. User identification (government-issued ID, plus name, date of birth, phone number, address, and email) — essential for fraud detection and law enforcement investigations; scammers often provide their own contact information to victims to enter at the kiosk.
4. Mandatory printed paper receipts — Not email only; paper receipts give law enforcement the wallet address, operator contact information, and transaction time, which can be critical in the first minutes of an investigation. Scammers commonly coach victims to delete digital receipts.
5. Kiosk location registration with the state — CSI estimates 400 machines in Montana; better data on where machines are located helps regulators and law enforcement.
6. Live customer service during operating hours.

7. Clearly disclosed fees and exchange rates — Many kiosks charge 25–35% in fees (one operator's terms allow up to 50%); fees are often hidden in fine print. Mainstream exchanges like Coinbase or Gemini charge approximately 2%.
8. Mandatory scam warning notices posted on or near the kiosk — A Nebraska law enforcement officer described a victim who saw the posted sign, called law enforcement, and was able to stop an $8,000 transaction.
9. Dedicated law enforcement contact line at the kiosk company — Operators had been ignoring law enforcement requests for transaction information needed to assist fraud victims; the law should require timely compliance with law enforcement requests.

Alternative Approach — Full Ban

While AARP did not begin with support for full bans, Ms. Flynt-Barr stated that as more data has come in and more attorneys general have conducted investigations, the data shows that in many communities the machines create an unacceptable, constant risk. AARP came out strongly in support of all three state bans enacted in 2026.

Evolution of the Cryptocurrency Kiosk Industry

- Increased focus on compliance and Know Your Customer (KYC) checks.
- Industry creating loopholes — e.g., the "app to cashier model," where a user brings cash to a store cashier and shows a QR code on a phone rather than using the kiosk machine directly. AARP has drafted model legislation to include this model within the definition of a kiosk operator.
- Increased state oversight and investigations from attorneys general across the country.
- Bitcoin Depot — formerly the largest kiosk operator in the U.S. with approximately 9,000 kiosks — filed for bankruptcy approximately two weeks prior to the meeting. In its press release, Bitcoin Depot cited increased state compliance requirements as a contributing factor. Ms. Flynt-Barr stated this suggests the company's profitability depended heavily on fraud victims.
- Montana has at least four additional kiosk operators beyond CoinFlip.

Public Comments — Fraud Victim Testimonies

Testimony of Tom Hopgood, Clancy, Montana

Mr. Hopgood, age 72, of Clancy, Montana, provided testimony detailing his personal experience as a cryptocurrency kiosk fraud victim. His remarks were based on contemporaneous notes made at or shortly after the events he described.

On January 8, 2026, Mr. Hopgood received a text message from an unknown number claiming that withdrawals had been "preauthorized" on his personal Wells Fargo checking account — to sites including childpornography.com and a gambling site. The message directed him to call a listed number to "rectify" the situation. He was connected to a person identifying himself as "Gary Anderson" from the Wells Fargo fraud desk. Operating under a sense of alarm and urgency, Mr. Hopgood followed the scammer's instructions.

Over the course of several days:

- He was directed to withdraw $4,800 from his personal Wells Fargo checking account and deposit it into a Bitcoin kiosk at the Green Meadow Market in Helena.
- The following day, he was told scammers had targeted a second Wells Fargo account he held in connection with the probate of a friend's estate. He was directed to withdraw $11,500 from that account and deposit it into a Bitcoin kiosk several doors down from the Wells Fargo branch.
- **Total loss:** $16,300.
- The scammer, while on the phone with Mr. Hopgood, remotely accessed his phone and deleted all communications, including texts and call history.

Mr. Hopgood stated that over the following months he learned how widespread this type of fraud is, and that he could not mention the incident to anyone without hearing of the same or similar experience having happened to them or their family members. He noted that Jefferson County law enforcement told him the money was not recoverable. He disputed the CoinFlip presenter's description of an easy refund process, stating that he received no refund and no information about one.

Mr. Hopgood stated that a close friend, Rob Freistadt, had almost exactly the same experience. He urged the Task Force to recognize this as a real and significant threat to Montanans, expressed confidence that members know the right course of action, and thanked the committee.

Testimony of Rob Freistadt, Helena, Montana

Mr. Freistadt, age 70, is mostly retired after careers in business and public school teaching. On a morning in May, he received a pop-up graphic on his computer appearing to indicate a security intrusion and directing him to call a support number. The caller, after presenting what appeared to be legitimate Microsoft credentials and badge numbers, claimed to have found child pornography on Mr. Freistadt's computer — something he had never accessed. Over an extended period, the scammer built a psychological environment of paranoia and trust. A second caller, impersonating a credit union fraud department representative, then raised concerns about one of Mr. Freistadt's financial accounts.

Mr. Freistadt was instructed to:

- Remove all funds from the targeted account and convert them to cash.
- Deposit the cash — **$16,000 in $100 bills** — into a Bitcoin kiosk at a gas station, after the first attempted location (a cannabis dispensary) was avoided because the scammer heard the store mention prior fraudulent transactions on their machine.
- The scammer stayed on the phone the entire time while Mr. Freistadt drove to the kiosk.

Mr. Freistadt reported that he grew suspicious only when the scammer asked for his home mortgage information, at which point his daughter-in-law intervened and demanded he hang up. He contacted the city police, a bitcoin company representative (who stated the money had likely already been collected and offered no further assistance), the Attorney General's office, and Commissioner Brown's office. He was unable to recover his funds.

He proposed, at a minimum, a 48-hour moratorium on allowing funds deposited into a Bitcoin kiosk to be collected by the recipient.

Mr. Freistadt noted that the credit union head teller who counted out his cash later told him her own mother had been scammed the same way — but made no mention of it at the time.

Response by Kirsten Madsen

Kirsten Madsen: Asked both Mr. Hopgood and Mr. Freistadt about their experience with the warning labels on the kiosk machines.

Mr. Freistadt: Stated that decals on the machine did warn about scams and that transactions are nonrefundable, but that in his state of paranoia he read the warnings as saying transactions were refundable. He also noted the text was very small and difficult to read without glasses, and that the scammers are "masterful at the use of psychology to build paranoia" — making it easy to overlook warnings.

Presentation: AARP Montana — Crypto Kiosk Fraud Fact Sheet and Model Legislation

Presenter: Kristin Page-Nei, AARP Montana Government Relations Director

Ms. Page-Nei thanked the fraud victims for their courage in sharing their stories and distributed: (1) A fact sheet summarizing the information presented by Ms. Flynt-Barr on cryptocurrency kiosk fraud; and (2) approximately five copies of AARP's model Virtual Currency Kiosk Fraud Prevention Bill (December 2025 version) for committee members.

Model Legislation Handout — Overview

Section 1 — Definitions
Defines "user," "virtual currency," "virtual currency address," "virtual currency wallet," "virtual currency kiosk," "virtual currency kiosk operator" (including those using app-to-cashier models), "virtual currency kiosk transaction," "blockchain analytics," "blockchain analytics and tracing software," and "charges."

Section 2 — Licensing and Reporting
Requires kiosk operators to be licensed as money transmitters; requires prior state approval for each kiosk location; requires quarterly location reports (including virtual currency addresses used and number of transactions declined for illicit activity suspicion) and annual reports (including gross revenue, complaints, total transaction volume, refund data, SARs filed, and compliance officer contact information); and requires operators to provide transaction data to regulators on request.

Section 3 — Disclosures
Requires clear, conspicuous disclosures in the user's chosen language; mandatory acknowledgment by user at each transaction; a bold warning that the technology can be used to defraud; disclosure of material risks (not government-backed, not FDIC/NCUA/SIPC protected); required display of operator

contact information and law enforcement contact information; mandatory paper and electronic receipts containing operator name, toll-free service number, law enforcement contact information, transaction type/value/date/time/virtual currency address/transaction hash, all charges, exchange rate, and refund policy.

Section 4 — Fraud and Money Laundering Prevention
Requires written anti-fraud and AML policy; mandatory use of blockchain analytics and tracing software to prevent transactions to known or likely fraudulent wallets; blocking transactions to overseas exchanges inaccessible to U.S. users; conspicuous posted written warning at or near the kiosk; government-issued ID verification for every transaction (operator strictly liable for violations); annual staff training for host location employees; and prohibition on using alternative methods (app-to-cashier, online portals) to evade transaction limits or other provisions.

Discussion

Commissioner Hall: Asked whether AARP has a preference between comprehensive regulation and an outright ban.

Ms. Page-Nei: Stated that AARP came out strongly in support of all three state bans enacted in 2026, but acknowledges political realities vary by state. She indicated AARP would ultimately support a ban and would work with anyone to achieve the most impactful legislation possible.

Trevor Graff (Government Affairs Director, Commissioner of Securities and Insurance): Stated that the CSI fully intends to bring at least one agency bill on this topic to the next legislative session. He noted the agency's thinking has evolved from a regulatory approach to potentially running a ban bill but confirmed the agency bill package will include at minimum the broad regulatory fixes discussed — and potentially a ban.

Senator Zolnikov: Requested that the CSI work with him and other legislators who have been working on these issues previously to ensure continuity and avoid duplication.

Mr. Graff: Confirmed the office is working with all willing partners and has not yet finalized the approach.

Sam Sill: Asked whether there is any downside to an outright ban.

Co-Chair Schomer: Said he could not think of one.

Leigh Drogen: Stated he saw no reason not to ban; the underlying technology and the industry as a whole are not served by these machines.

Alex Miller: Said he would want the ban language to be carefully crafted to avoid unintended second-order effects on legitimate uses, noting the transaction fees of 15–20% are "offensive" even for legitimate transactions.

Co-Chair Schomer: Expressed personal support, noting he could not see any value to the kiosk machines and stating that legislators have an obligation to protect people first and foremost. He expressed confidence that the issue will be addressed through legislation, whether through an outright ban or very strict regulations.

Break

The meeting recessed briefly.

Presentation: Rocky Mountain Information Network — Law Enforcement Perspective on Cryptocurrency Fraud

Presenter: Tom Pallach, Law Enforcement Coordinator, Rocky Mountain Information Network (RMIN)

Mr. Pallach retired from Gallatin County law enforcement after 28 years of service, specializing in a wide range of crimes including cyber and financial crimes. RMIN is one of six regional nodes of the RISS network (Regional Information Sharing Systems), a program created in 1974 (Montana joined in 1977) to provide intelligence, analytical, and officer safety support to law enforcement, funded by the U.S. Department of Justice. RMIN's primary mission is to break down jurisdictional boundaries in criminal investigations.

Montana Cryptocurrency Crime Statistics — RMIN Data

- 2025: $1.5 million in cryptocurrency crime losses, 15 cases investigated or assisted by RMIN.
- 2026 (to date): 4 cases, $113,000 in losses.
- 2025 through present total: $1.6 million.
- Types of crime range from theft of seed cards to cryptocurrency scams.

FBI IC3 Data for Montana (2025)

- Three top scam categories for 2025 financial crimes: (1) confidence/romance (pig butchering); (2) investment; (3) tech support.
- Montana losses: $22 million (crypto wallet-related) + $12 million (additional cryptocurrency losses) = more than $34 million total in cryptocurrency crimes in 2025.
- By age group: Adults 60+ suffered approximately $21 million; adults 20–29 suffered approximately $300,000.
- 69 crypto kiosk complaints, $1.5 million in losses (acknowledged as a significant undercount due to underreporting and embarrassment).

Mr. Pallach noted that the CSI office also has had 5 Bitcoin ATM cases in 2026 to date, totaling $149,000 in losses reported to their office.

Kirsten Madsen added that the FBI IC3 data shows $17 million in investment fraud losses from Montana in 2025 — money she characterized as capital that should have gone to legitimate investments and businesses in Montana, and whose loss hinders the state's economy.

Types of Scams Being Seen

- Web-based pop-up scams (social media and email phishing)
- Phone call scams — the dominant cryptocurrency kiosk scam type
- Common typologies: "lonely heart" romance scams; sex offender impersonation (claiming the victim has been found browsing child pornography); jury summons impersonation; government impersonation; bond payment for a relative in custody.

The Georgia State Prison Connection

Mr. Pallach explained that many of the phone call scams originate from Georgia state prisons, specifically run by the Blood prison gang. He shared intelligence from the Georgia Department of Corrections intelligence officer:

- Gangs recruit well-spoken, persuasive individuals within prisons specifically to run scam operations.
- Prison scammers have access to an "intel research division" that performs data mining using tools such as LexisNexis, TLO, Zillow, and Realtor.com to identify and target high-value households (using real estate values as a proxy).
- Scammers identify the names of local law enforcement officers — detectives, sergeants — and impersonate them to lend credibility to scam calls.
- The Georgia DOC intelligence officer told Mr. Pallach that these crimes are making murderers and rapists serving life sentences into millionaires.
- Cell phones are smuggled into prisons via drones, through smuggling by correctional staff, or other means.
- He cautioned agencies to contact the Georgia Department of Corrections directly, not individual prison facilities, when investigating calls traced to Georgia.

Blockchain Tracing Challenges

Mr. Pallach showed a partial blockchain trace exhibit from a Georgia state prison-related case. The trace, which represented only one-eighth of the full document, showed a complex web of transactions with a cluster in the upper right representing cash-out activity. He described the difficulty as follows:

- Open-source tracing tools are slow, cumbersome, and often inadequate.
- Montana has hosted two training sessions — one for prosecutors and one for law enforcement — using TRM Labs and Chainalysis tracing tools. However, these tools are expensive and out of reach for most Montana agencies.
- RMIN has access to blockchain analytics tools and can perform tracing on behalf of local and county agencies upon request.
- TRM Labs reported approximately 1.2% of total kiosk transactions are scam-related, putting industry figures in context.
- CoinATM Radar shows CoinFlip's transaction fee at 18.9%. Bitcoin Depot — one of the previously cooperative companies on refunds — has now filed for bankruptcy.

Law Enforcement Coordination Challenges

In response to Commissioner Hall's question about coordination among city, county, state, and federal agencies, Mr. Pallach stated that the system is not working well and that there is currently no cohesive enforcement approach to cryptocurrency crimes in Montana. Different agencies reach different dead ends. Some contact RMIN; others contact state agencies; many do not seek help at all.

He mentioned REACT and the Shamrock network — a nationwide email listserv for law enforcement handling technological and cryptocurrency crimes — as a resource for sharing information and expertise.

He suggested that a multi-jurisdictional task force focused on cryptocurrency crimes, to which all such cases would automatically be routed, would be beneficial given the specialized nature of the investigations.

Law Enforcement Recommendations

Mr. Pallach stated clearly that his view is that the removal of cryptocurrency ATM kiosks from Montana would be the single most impactful action the state could take. In his professional assessment: "I just want those things gone, and I think that would save a bunch for everybody."

He also emphasized the critical importance of public education, urging a public awareness approach analogous to drug prevention education — educating people that no government or bank will ever ask for payment in cryptocurrency, and raising awareness of common scam typologies. He drew an analogy to the history of financial crime, noting that in 2016 the same criminal networks ran similar operations using gift cards; when those became regulated, they moved to cryptocurrency kiosks. "As soon as we get this figured out, they're going to get something else."

Discussion

Senator Zolnikov's DOJ Technology Bill

Senator Zolnikov: Mentioned that the Energy and Technology Committee has approved a bill funding the DOJ to acquire blockchain tracing technology to assist in the seizure and recovery of scammed cryptocurrency. He noted the appropriation request is approximately $500,000 (one-time only), and that victim testimony — like that heard today — is critical to passing it.

Discussion on Asset Seizure Laws

Chris McConnell: Asked whether updating Montana's asset forfeiture and seizure laws — currently structured around drug seizures — would help law enforcement.

Mr. Pallach: Confirmed the laws are antiquated with respect to financial and cryptocurrency crimes but noted that some large exchanges like Binance are willing to freeze assets at the request of law enforcement on letterhead alone, without waiting for a court order. He noted RMIN has published guidance on what each major exchange requires to freeze and seize assets. However, he acknowledged that no Montana agency has yet formally seized cryptocurrency, and that establishing a government

cryptocurrency wallet — a necessary prerequisite for seizing and holding digital assets — should occur proactively, before a seizure is attempted.

Co-Chair Schomer: Thanked Mr. Pallach and expressed interest in convening a working group with law enforcement, DBFI, and CSI to find proactive, forward-looking solutions to cryptocurrency crimes, rather than continually reacting after the fact.

Working Session

Status of the Task Force

Commissioner Hall noted that this was the final scheduled meeting of the Task Force. The office has already begun work on condensing the Task Force's meetings and materials into a report. As directed under Senate Bill 330, the Task Force is required to produce a report of its work to the Economic Affairs Interim Committee (EAIC).

Next Steps — Report Process

- DBFI will draft a report that presents ideas and frameworks considered by the Task Force without necessarily making specific legislative recommendations. The goal is to lay out options and considerations for the EAIC.
- Commissioner Hall indicated a draft will be provided to Co-Chairs within approximately two weeks, after which it will circulate to the full Task Force for comments and feedback.
- Task Force members who wish to ensure a particular topic, concern, or recommendation is included in the report are encouraged to email Commissioner Hall directly.
- If the EAIC has questions or requests additional work after reviewing the report, or if significant new developments occur (such as finalization of GENIUS Act federal rules), the Task Force may reconvene in the fall by agreement of the co-chairs.

Request for Data on Montana's Blockchain/Cryptocurrency Industry

Commissioner Hall requested that any Task Force member with information on the size and scope of Montana's blockchain and cryptocurrency business community share it with her office, noting she does not have a clear picture of how many businesses in the state are meaningfully engaged in this sector. She suggested that Task Force members including Tanner Avery, Alex Miller, Julie Fredrickson, Daniel Pittman, and Leigh Drogen may have relevant insights. This information would provide important context for the report.

Discussion

Co-Chair Schomer: Stated that while the Task Force was "wading through murky water," the process had been very good, very informative, and produced good material for potential legislation.

Senator Zolnikov: Noted that Senator Morigeau should be included in future bill-drafting conversations on crypto kiosk legislation, as he would be a good candidate to carry related legislation.

Senator Morigeau: Confirmed his willingness to carry bills as needed.

Sam Sill: Offered thanks on behalf of the committee to both co-chairs and to Commissioner Hall, Heather Bernet, and DBFI staff for their work preparing and managing the Task Force process.

Public Comment

Kristin Page-Nei, AARP Montana

Ms. Page-Nei noted that AARP is tracking a number of fraud-related bills at the federal level and has endorsed approximately 30 of them. She highlighted several of potential interest to the Task Force:

1. GUARD Act (HR 2978 / SB 2544) — Ensuring law enforcement has the right tools and training to fight fraud and scams. Representative Downing (Montana) is a co-sponsor.
2. Stop Scams Against Seniors Act — Consumer protection focused.
3. AI Fraud Accountability Act (SB 3982 / HR 7786) — Senator Sheehy (Montana) is a lead sponsor.

Ms. Page-Nei provided a full list of AARP-endorsed federal bills to Heather Bernet for distribution to the committee.

Adjournment

Co-Chair Schomer thanked all members, presenters, and the public for attending, acknowledged the significant effort contributed by all participants, and adjourned the meeting at 12:34 pm MST.

Materials Submitted/Distributed at Meeting

- DBFI Presentation — Stablecoins and the GENIUS Act
- CoinFlip Presentation — Montana Blockchain & Digital Innovation Task Force Presentation
- AARP Presentation — Cryptocurrency Kiosk Fraud Prevention
- RMIN Presentation — Cryptocurrency Fraud and Law Enforcement Perspective
- AARP Handout — Virtual Currency Kiosk Fraud Prevention Bill
- AARP Handout — AARP is Fighting to Stop Criminals from Stealing Over $389 Million a Year
- CSI Handout — Investment Fraud in Montana
- CSI Handout — Montana Scam Stats
- AARP Federal Bill Tracking List