

**2025 HOUSE INDUSTRY, BUSINESS AND LABOR**

**HB 1447**

# 2025 HOUSE STANDING COMMITTEE MINUTES

## Industry, Business and Labor Committee Room JW327C, State Capitol

HB1447  
1/22/2025

A BILL for an Act to create and enact a new chapter to title 54 of the North Dakota Century Code, relating to the advanced technology review committee, advanced technology grant program, and advanced technology grant fund; to provide for a transfer; and to provide an appropriation.

10:17 a.m. Chairman Warrey opened the meeting.

Members Present: Chairman Warrey, Vice Chairman Ostlie, Vice Chairman Johnson, Representatives Brown, Finley-DeVille, Grindberg, Kasper, Koppelman, D. Ruby, Schatz, Schauer, Vollmer. Member Absent: Representative Bahl.

Member Absent: Representative Christy.

### Discussion Topics:

- Virtual currency kiosks
- Krypto machine
- Fraud warning notices
- Paper receipt
- Operator's refund
- Model legislation in some States
- Map kiosks in ND
- 5.6 billion in fraud
- Daily transaction limitation
- Anti money laundering

10:17 a.m. Representative Steve Swointek, District 10, Fargo, ND, introduced and testified.

10:25 a.m. Josh Askvig, State Director, AARP North Dakota, testified in favor and submitted testimony #30578, #30579 and #30580.

10:39 a.m. Lise Kruse, Commissioner, ND Department of Financial Institutions, testified in favor and submitted testimony #30594.

11:03 a.m. Rick Clayburgh, President/CEO, ND Bankers Association, testified in favor and submitted testimony #30613.

11:10 Jacob Rud, Fraud Investigator, First Western Bank, testified in favor and submitted testimony #30762.

11:24 a.m. Lacey Bjork Anderson, The Birch Group LLC, testified in opposition.

11:28 a.m. Ethan McClellan, Director of Government Relations, Bitcoin Depot, testified in opposition and submitted testimony #30665.

11:41 Kevin Lolli, Assistant General Counsel, CoinFlip, submitted testimony in opposition #30655

**Additional Written Testimony:**

Elin S. Alm, Director Consumer Protection and Antitrust Division, Office of the Attorney General, submitted testimony in favor #30638.

John Alexander, Dakota Credit Union Association (DakCU), submitted testimony in favor #30795.

11:47 a.m. Chairman Warrey closed the meeting.

*Diane Lillis, Committee Clerk*



cryptocurrency atm

Bismarck



Map data ©2025 Google 1 mi

Hours ▼


**≡ All filters**

## Results ⓘ

**Sponsored**

## Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM ·  · 706 Kirkwood Mall

Opens soon · 11AM ·

(678) 435-9604



Website



### Directions

## Locate The Closest Bitcoin ATM

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM locations**....

[Visit Site](#)

**Sponsored**

## RockItCoin Bitcoin ATM

No reviews

Crypto ATM ·  · 2921 N 11th St



Website



### Directions



Open · Closes 11 PM ·

(888) 702-4826

### BTC ATM

Use "EARN10" Promo Code at RockItCoin®

**ATMs** & Earn an Extra \$10 Bitcoin in Your...

[Visit Site](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 1144 E Bismarck Expy

Open · Closes 12 AM · (701) 401-3888



[Directions](#)

### Cryptobase Bitcoin ATM

No reviews

ATM · [📍](#) · 406 N 6th St

Open 24 hours · (301) 702-0115



[Website](#)



[Directions](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 4400 Ottawa St

Open · Closes 12 AM · (701) 401-5286



[Directions](#)

### LibertyX Bitcoin ATM

No reviews

ATM · 406 N 6th St

Open 24 hours · (800) 511-8940



[Website](#)



[Directions](#)

### Bitcoin ATM Bismarck-Cryptobase

No reviews

ATM · [📍](#) · 4100 Saratoga Ave

Open 24 hours · (305) 702-0115



[Website](#)



[Directions](#)

### Coinstar Kiosk - Bitcoin ATM

No reviews

ATM · [📍](#) · 1144 E Bismarck Expy

Coborn's

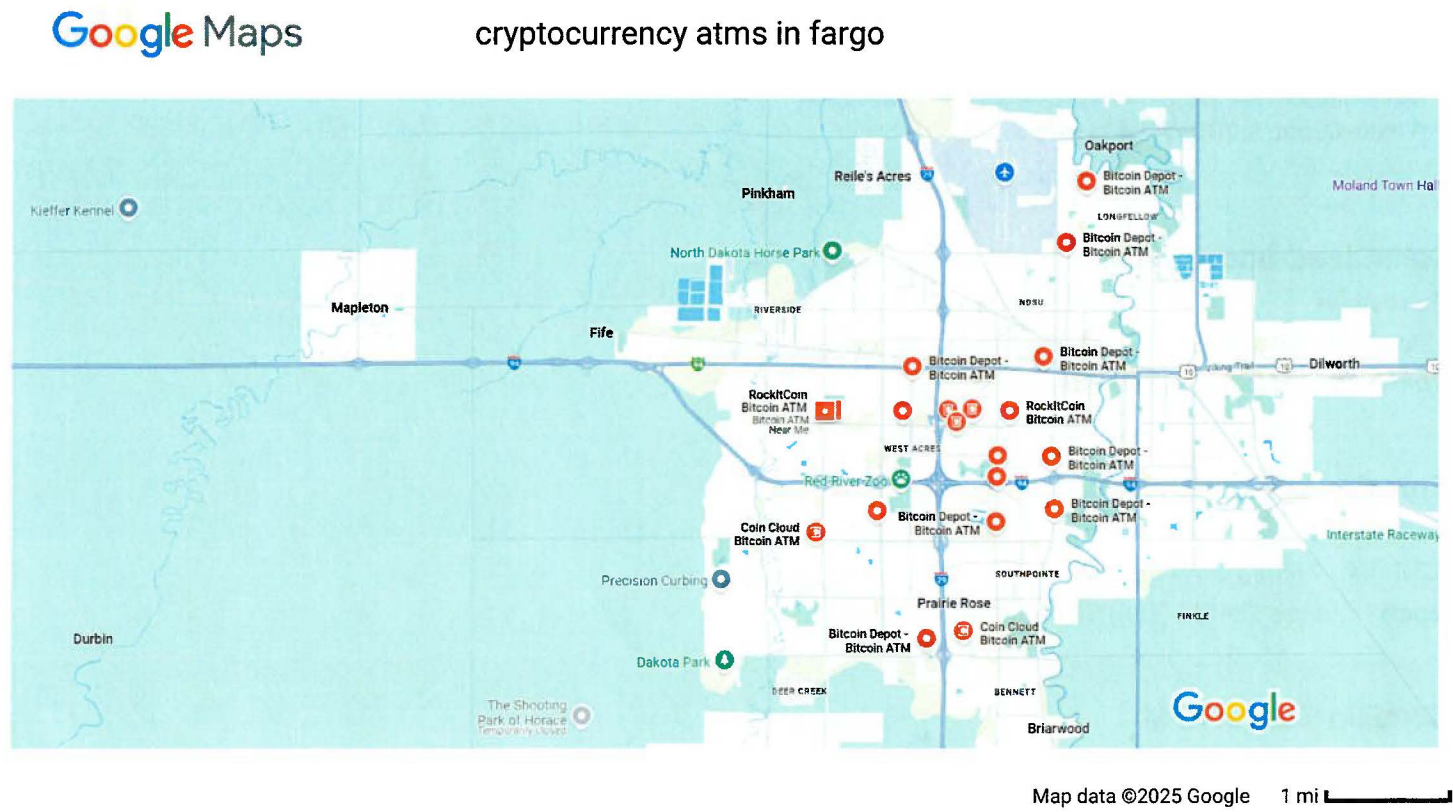
Open · Closes 5 PM ·



[Website](#)



[Directions](#)



Hours ▾

🔍 All filters

Results ⓘ

Showing results for **cryptocurrency** atms in fargo. Search instead for **cyrpotcurrency** atms in fargo.

Sponsored

RockItCoin Bitcoin ATM

3.0 (1)

Crypto ATM · 📍 · 950 13th Ave E

Open 24 hours · (888) 702-4826





Website

Directions

Bitcoin ATM Near Me

Use "EARN10" Promo Code at RockItCoin® ATM & Get Extra \$10 of Bitcoin on...


Visit Site


Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 📍 · 1210 13th Ave E





Website

Directions

Open 24 hours · (678) 435-9604

**15,000+ Locations Nationwide**

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM** locations. 24...

[Visit Site](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 1401 33rd St S

Open · Closes 12AM · (218) 789-8292



[Directions](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 📍 · 755 33rd Ave E

Open · Closes 12AM · (701) 929-6588



[Directions](#)

### CoinFlip Bitcoin ATM

5.0 (3)

ATM · 📍 · 3021 13th Ave S Unit 1

Open · Closes 9 PM ·

(773) 800-0106



[Website](#)



[Directions](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 4907 Timber Pkwy S

Open · Closes 12AM · (701) 369-9740



[Directions](#)

### Coinsource Bitcoin ATM

No reviews

ATM · 📍 · 3441 13th Ave S

Open · Closes 9 PM ·

(805) 500-2646



[Website](#)



[Directions](#)

### Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 📍 · 3040 25th St S

Open 24 hours · (678) 435-9604



[Website](#)



[Directions](#)



cryptocurrency atm near Dickinson nd



Map data ©2025 Google 2000 ft

Hours ▾

All filters


Results ⓘ

Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews  
Crypto ATM · 797 S Main Ave  
Open · Closes 10 PM ·  
(678) 435-9604

  
Website

  
Directions

Bitcoin ATM Promo Code

New Customer Promo Special! Buy Bitcoin with Cash at over 15,000+ Bitcoin Depot... [Visit Site](#)

Sponsored

Byte Federal Bitcoin ATM (Arco)

5.0 (2)  
Crypto ATM ·  · 450 12th St W

  
Website

  
Directions



**Bitcoin ATM Locations Near You**

Bitcoin **ATM Near Me** - Search for the  
USA's Best Crypto **ATMs** - Highest Limits...

[Visit Site](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 📍 · 1761 3rd Ave W

**Open** · Closes 11PM · (701) 502-4647

[Directions](#)**Byte Federal Bitcoin ATM  
(Arco)**

5.0 (2)

Crypto ATM · 📍 · 450 12th St W

**Open** · Closes 10 PM ·

(786) 686-2983

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 797 S Main Ave

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 191 40th St W

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 1005 E Villard St

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Coinstar Kiosk - Bitcoin ATM**

3.0 (2)

ATM · 📍 · 1761 3rd Ave W Coborn's

**Open** · Closes 10 PM ·

(800) 928-2274

[Website](#)[Directions](#)



cryptocurrency atm near minot, nd



Map data ©2025 Google 1 mi

Hours ▾

All filters

## Results ⓘ

Showing results for **cryptocurrency** atm near minot, nd. Search instead for **cryptocurrency** atm near minot, nd.

## Sponsored

**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 🚶 · 1512 4th Ave NW

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

**15,000+ Locations Nationwide**Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM** locations. 24...[Visit Site](#)

## Sponsored

**RockItCoin Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 2025 3rd St NW

**Open** · Closes 8 PM ·

(888) 702-4826

[Website](#)[Directions](#)**Bitcoin ATM Near Me**

Use "EARN10" Promo Code at RockItCoin®

[Visit Site](#)

ATM &amp; Get Extra \$10 of Bitcoin on...

**Bitcoin Depot - Bitcoin ATM**

5.0 (1)

Crypto ATM · 📍 · 301 40th Ave SW

**Open** · Closes 11 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Coinsource Bitcoin ATM**

5.0 (1)

ATM · 1520 24th Ave SW

**Open 24 hours** · (805) 500-2646[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 1512 4th Ave NW

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 409 E Burdick

Expy

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 810 N Broadway

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 2400 10th St SW

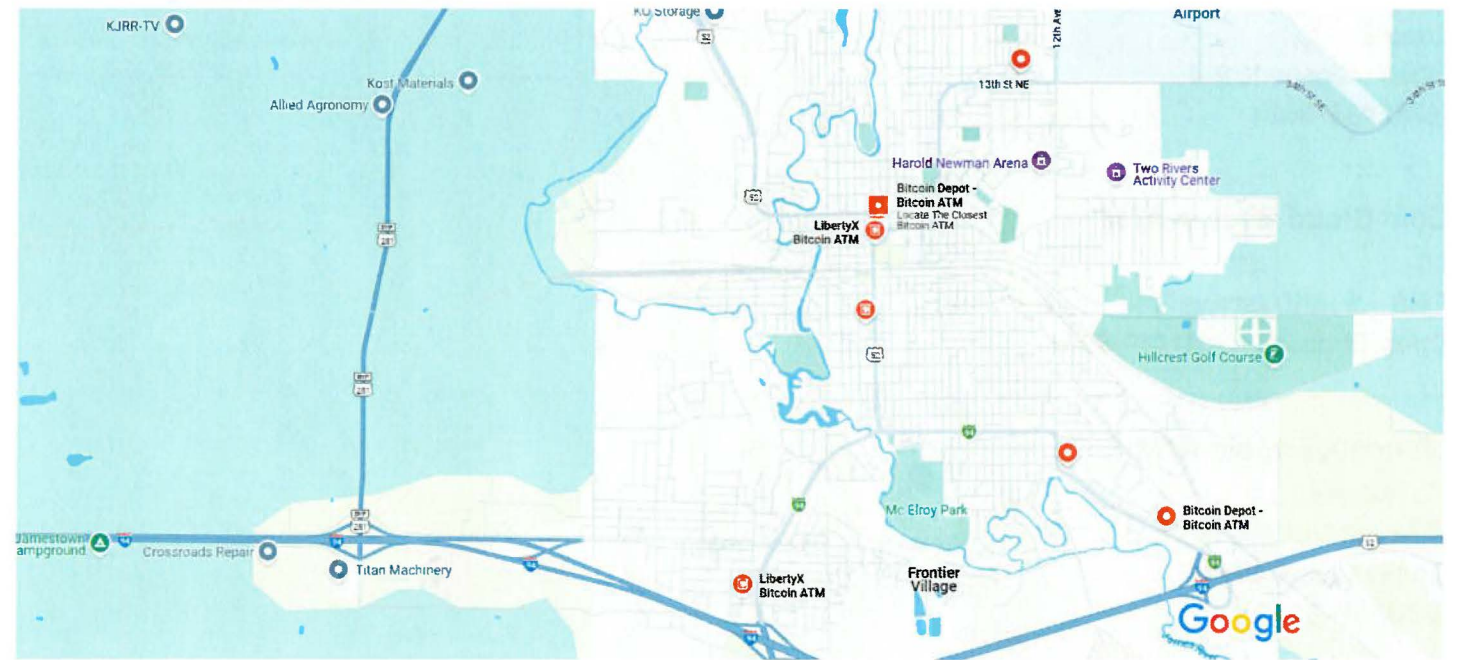
**Open** · Closes 7 PM ·

(678) 435-9604

[Website](#)[Directions](#)



cryptocurrency atm near jamestown, nd



Map data ©2025 Google 2000 ft

Hours ▾

🔍 All filters

Results ⓘ

Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 424 1st Ave N

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

Locate The Closest Bitcoin ATM

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ ATM locations. 24...

Visit Site

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 424 1st Ave N

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions



**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 1609 Business Loop E

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Coin Cloud Bitcoin ATM**

1.0 (1)

ATM · 📍 · 310 1st Ave S

**Open 24 hours** · (701) 419-8894[Website](#)[Directions](#)**LibertyX Bitcoin ATM**

No reviews

ATM · 424 1st Ave N

**Open** · Closes 10 PM ·

(800) 511-8940

[Website](#)[Directions](#)**LibertyX Bitcoin ATM**

No reviews

Crypto ATM · 1219 Business Loop E  
(800) 511-8940[Directions](#)**Buy Bitcoin**

No reviews

Crypto ATM · 📍 · 1003 13th St NE  
(888) 212-5824[Website](#)[Directions](#)**Buy Bitcoin**

No reviews

Crypto ATM · 📍 · 1219 Business Loop E  
(888) 212-5824[Website](#)[Directions](#)



cryptocurrency atm near grand forks, nd



Map data ©2025 Google 2000 ft

Hours ▾

🏠 All filters

Results ⓘ

Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 4250 University Ave

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

Locate The Closest Bitcoin ATM

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM** locations. 24...

Visit Site

Sponsored

CoinFlip Bitcoin ATM

1.0 (1)

ATM · 🚶 · 4220 5th Ave N

Open · Closes 11 PM ·

(773) 800-0106



Website



Directions

**Coin Cloud Bitcoin ATM**

5.0 (1)

ATM · 🚶 · 1750 32nd Ave S

**Open** · Closes 10 PM · (701) 987-3073[Directions](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 🚶 · 1631 S Washington St

**Open** · Closes 10 PM · (701) 765-5004[Directions](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 🚶 · 1315 S Columbia Rd

**Open** · Closes 10 PM · (701) 765-5298[Directions](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 🚶 · 1925 13th Ave N

**Open** · Closes 10 PM · (701) 402-5582

Onsite services

[Directions](#)**Bitcoin Depot - Bitcoin ATM**

1.0 (1)

Crypto ATM · 🚶 · 3450 32nd Ave S

**Open 24 hours** · (678) 435-9604[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 4326 Gateway Dr

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)

[REDACTED],

I know that calling [REDACTED] or visiting XXXX [REDACTED] Drive would be an effective way to have a chat with you in case you don't act. Don't even try to escape from this. You've no idea what I'm capable of in Bismarck.

It's important you pay attention to this message right now. Take a moment to chill, breathe, and analyze it thoroughly. 'Cause we're about to discuss a deal between you and me, and I ain't playing games. You do not know anything about me however I know ALOT about you and you must be thinking how, correct?

Well, you've been treading on thin ice with your browsing habits, clicking through those girlie videos and venturing into the darker corners of cyberspace. I installed a Malware on a porn website & you accessed it to watch (know what I mean?). When you were busy watching those videos, your device started out functioning as a RDP (Remote Control) which provided me with complete control over your device. I can peep at everything on your display, flick on your cam and mic, and you wouldn't even notice. Oh, and I've got access to all your emails, contacts, and social media accounts too.

Been keeping tabs on your pathetic existence for a while now. It's simply your bad luck that I noticed your blunder. I gave in more days than I should've digging into your data. Extracted quite a bit of juicy info from your system. and I've seen it all. Yeah, Yeah, I've got footage of you doing filthy things in your room (nice setup, by the way). I then developed videos and screenshots where on one side of the screen, there's whatever garbage you had been enjoying, and on the other part, it's someone jerking off. With just a click, I can send this filth to all of your contacts.

Your confusion is clear, but don't expect sympathy. Wholeheartedly, I am ready to wipe the slate clean, and let you continue with your regular life and forget you ever existed. I will offer you two options. Alternative one is to ignore my e mail. Let us see what is going to happen if you pick this option. I will send your video to all of your contacts. The video is lit, and I can't even fathom the humiliation you'll face when your colleagues, friends, and fam see it. But hey, that's life, ain't it? Don't be playing the victim here.

Second option is to pay me, and be confidential about it. We will call this my "privacy fee". Now let me tell you what happens when you select this choice. Your dirty secret will remain private. I will destroy all the data and evidence once you come through with the payment. You need to make the payment through Bitcoins only. I want you to know I'm aiming for a win-win here. I stand by my promises.

**Amount to be paid:** USD 1950

**BTC ADDRESS IS:** bc1q2jz2eavj0htw8m68u6evs950x5cztwx6dls4n5

Once you pay up, you'll sleep like a baby. I keep my word.

**Pay Attention:** You have one day in order to sort this out and I will only accept Bitcoin. I've a special pixel in this e mail, and right now I've been notified that you have read through this e mail. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the complete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I catch that you've shared or discussed this email with someone else, your shitty video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings, I already have all your data. I don't make mistakes, [REDACTED].

Honestly, those online tips about covering your camera aren't as useless as they seem. Now, I am waiting for my payment..



House Bill 1447 – Support  
January 22, 2025  
House Industry, Business and Labor Committee  
Josh Askvig, AARP ND- [jaskvig@aarpp.org](mailto:jaskvig@aarpp.org)

Chairman Warrey and members of the House Industry, Business and Labor Committee,  
My name is Josh Askvig, State Director with AARP North Dakota. AARP is a nonpartisan, nonprofit, nationwide organization with nearly 38 million members. Approximately, 82,000 of those members live in North Dakota.

Scams involving cryptocurrency ATMs are on the rise—and AARP ND is urging you to take action this legislative session. HB 1447, sponsored by Representative Swiontek, will create important consumer protections to save older North Dakotans from having their hard-earned money, sometimes their life savings, stolen by criminals misusing crypto kiosks or “ATMs” for fraudulent activity.

Cryptocurrency fraud has taken a quantum leap in recent years. The FBI says that in 2023, Americans reported losing more than \$5.6 billion through fraud involving cryptocurrency, North Dakotans lost over \$6 million in cryptocurrency fraud. One area of growth is in payments using cryptocurrency ATMs, also known as “crypto kiosks” or “virtual currency kiosks.” These devices can be found in supermarkets, convenience stores, gas stations, bars, restaurants, and shopping malls. Today, there are more than 45,000 crypto ATMs nationwide. Attached to the testimony are maps of where some of these machines are located in North Dakota.

Because crypto ATMs are still relatively new and largely unregulated at the state level compared to traditional financial institutions and money service businesses, they lack sufficient consumer fraud protections. As a result, criminals are using crypto ATMs to steal hundreds of millions of dollars from Americans each year through fraudulent purchase schemes. In the same report referenced above 2023, the FBI received over 5,500 complaints involving crypto kiosks, and Americans reported over \$189 million in stolen funds. Fraud is significantly underreported, so the amount stolen is likely far higher.

Perpetrators convince individuals that they must address an urgent matter, directing them to withdraw large amounts of cash from their banks. The individual then inserts that money into a crypto “ATM” and is told to direct the money to a “secure wallet.” Once the payment is made it’s transferred to the criminal and virtually untraceable. We have included a copy of one email we recently received directing a local Bismarck resident to keep some internet searches private by

making a payment at a cryptocurrency kiosk. This resident understood the warning signs and shared the email so we could help others.

As Representative Swiontek mentioned in his testimony, HB 1447 is designed to prevent North Dakotans from losing their savings to criminals by implementing important consumer protections including:

- **Licensing cryptocurrency kiosk operators in the state.** This is accomplished in section 1 of the bill specifically starting on page 2 line 17. Currently, North Dakota statute could use some clarity on requiring cryptocurrency kiosk operators to be licensed in North Dakota. This section would make it clear that they require licensure under the ND Department of Financial Institutions as a money transmitter. It also ensures that operators locate the kiosks in commercial areas and submit quarterly reports.
- **Posting fraud warning notices that are visible and identify steps people should take if they suspect fraudulent activity.** Because these crypto kiosks can look like bank ATMs, including disclosures and warnings is an important consumer protection. The language on page 3 lines 18-31 and page 4 lines 1-10, outline the notice that operators would be required to post and prompts to notify law enforcement if they suspect fraud. Additional disclosure requirements are on page 4 lines 11-30.
- **Clearly displaying terms and conditions before a transaction, including any fees charged and the exchange rate.** You can find these requirements spelled out on page 5 lines 8-22.
- **Fee caps.** Page 7, lines 24-31 provides that kiosk may not charge more than the higher of \$5 or 3% fee on transactions.
- **Giving paper receipts with relevant transactional information.** Page 5 lines 24-30, and lines 1-10 on top of page 6 make it clear that crypto kiosk operators must provide paper receipts with the operator's name and contact information, relevant state and local law enforcement in which to report fraud, the transaction details like sender and recipient names, transaction values and data, fee amounts. These and the other items aid law enforcement being able to investigate immediately, helping in victim recovery efforts.
- **Requiring cryptocurrency operators to refund ATM fees for fraudulent transactions related to fraud.** These requirements are spelled out on page 6, lines 11-31 and page 7, lines 1-18.
- **Imposing daily transaction limits to avoid potential risks associated with higher transactions.** Page 7, lines 20-23 specifies a \$1,000 limit on daily transactions per vendor. Currently, we are unaware of daily limits on transactions using cryptocurrency kiosks and we've been made aware of North Dakotans that have lost as much as \$25,000 in one transaction.

AARP regularly provides free timely information to consumers and their families through the work of our AARP Fraud Watch Network ([aarp.org/fraud](http://aarp.org/fraud)). In North Dakota alone, we regularly provide consumer updates via media partnerships, free shredding events, educational community events, telephone townhalls, webinars, and volunteer presentations. We also support laws and regulations that strengthen and enhance consumer protections, like those contained in HB 1447.

Fraud and other financial crimes, including cryptocurrency kiosk/ATM fraud, create real financial devastation —billions of dollars are lost each year. The impact of fraud on victims and their families is wide reaching and emotionally devastating, especially for older Americans. It's a crime that deserves more attention and effort to combat. **AARP North Dakota strongly supports protections against fraud and we urge you to support HB 1447.**

Thank you.



## MEMORANDUM

**DATE:** January 22, 2025

**TO:** House Industry, Business and Labor Committee

**FROM:** Lise Kruse, Commissioner

**SUBJECT:** Testimony in Support of House Bill No. 1447

Chairman Warrey and members of the House Industry, Business and Labor Committee, thank you for the opportunity to testify in support of House Bill No. 1447.

Our department oversees banks, credit unions, trust companies, and other nonbank financial corporations such as money transmitters and lenders. The department is in support of this Bill since it clarifies an area where we already have jurisdiction. We are asking that an amendment to the Bill be adopted, moving it into NDCC 13-09.1, where the oversight of virtual currency money transmitters is outlined. The department had already planned on expanding and clarifying that section, related to crypto ATMs, and therefore we were pleased to work with AARP on this topic.



We would request an amendment to move this Bill to 13-09.1. That is where our jurisdiction for virtual currency is already established and would therefore include any enforcement authority that is already established in current law. The changes would include adding the definitions under 13-09.1-44 and the remaining sections would then start at 13-09.1-50.

There has been an increase in fraud in recent years, and banks have alerted me to the increase in financial elder abuse, and now specifically, how grandma is duped into putting cash into a crypto ATM, often with help from the fraudsters, and the money is gone. Crypto ATMs have become the new avenue for fraudsters, instead of gift cards which was the fraudsters' currency of choice, this is faster since the cash loaded into a crypto ATM is instantaneously in the fraudster's crypto wallet. Due to the potential for fraud, I believe it is appropriate to enforce some type of limit, better consumer alerts at the machines, and clarify what the ATM owners are required to do to help prevent fraudulent transactions.

Per the FBI Internet Crime Complaint Center, total crypto fraud losses jumped 45% in 2023 to \$5.6 billion. The center reported over 69,000 complaints, with 17,000 complaints from people over the age of 60, with losses of \$1.6 billion. North Dakota complaints totaled 103 with \$6.5 million in losses, which is over \$60,000 per person on average. In the FBI report,

Crypto ATMs accounted for more than 5,000 complaints with losses of \$189 million. Over half the complaints were from individuals over the age of 60 and resulted in \$124 million of the losses. These numbers are likely low, since many victims, especially in our elderly population, are hesitant to report it due to embarrassment. A reason why the fraud victims with crypto ATMs are predominantly elderly is likely due to the fact that younger individuals active in the crypto marketplace uses exchanges on their phone and would not need a physical location.

Mr. Chairman, thank you for the opportunity to provide this testimony. I would be happy to answer any questions the Committee may have.



## Written Testimony in Support of HB 1447: Virtual Currency Kiosk Fraud Prevention

---

Chairman Warrey and Members of the Committee,

For the record, I am Rick Clayburgh, President and CEO of the North Dakota Banker's Association. The NDBA supports the enactment of House Bill 1447, which proposes to regulate crypto-currency kiosk machines here in North Dakota. NDBA supports HB 1447 because it will enhance consumer protection and maintain the integrity of our financial system.

Crypto-currency kiosks, often referred to as Bitcoin ATMs, have seen rapid growth in recent years. At the same time, Bitcoin ATM scams have led to significant consumer financial losses. According to the Federal Trade Commission (FTC), consumers reported losing over \$110 million to such scams in 2023. In the first half of 2024 alone, reported losses exceed \$65 million. These scams often involve fraudsters impersonating government officials, businesses, or tech support, creating a sense of urgency that prompts victims to withdraw cash and deposit it into Bitcoin ATMs.

Notably, the term "ATM" is misleading, as crypto-currency kiosks are not ATMs. ATMs are federally regulated and carry various protections for users. Many people using crypto-currency kiosks are misled into thinking they are protected when the fact is they are not.

HB 1447 aims to address the misuse of crypto-currency kiosks as tools for committing financial crimes with provisions such as:

1. **Licensing and Registration Requirements:** Prohibits kiosk operators from engaging in virtual-currency business activity absent a money transmitter license, which must be renewed annually. Kiosks must also be approved and registered.
2. **Disclosures:** Requiring certain disclosures to customers, including specific fraud and risk acknowledgments.
3. **Fraud Prevention:** The bill further requires operators to use specific software to assist in the prevention of fraud.
4. **Daily Transaction Limits:** Prohibits operators from accepting transactions of more than \$1000 per day in connection with a single customer.
5. **Fee Caps:** Limits the fees able to be collected by operators in connection with kiosk transactions.

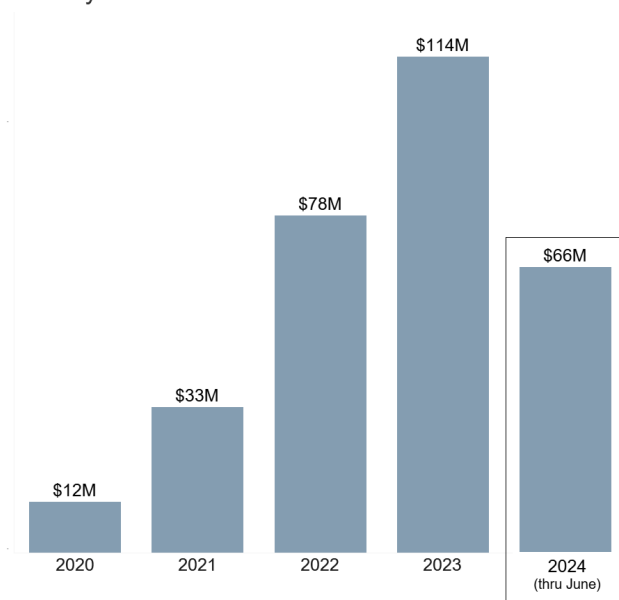
The regulation of crypto-currency kiosks is a necessary step to ensure that the rapid growth of digital asset platforms does not further compromise consumer protection, legal compliance, or financial stability. Crypto-currency kiosk operators will be held to a standard designed to empower consumers to make informed decisions, thereby fostering trust and collaboration within the financial ecosystem of our state.

## Bitcoin ATMs: A payment portal for scammers

Bitcoin ATMs (or BTMs)<sup>1</sup> have been popping up at convenience stores, gas stations, and other high-traffic areas for years.<sup>2</sup> For some, they're a convenient way to buy or send crypto, but for scammers they've become an easy way to steal. FTC Consumer Sentinel Network data show that fraud losses at BTMs are skyrocketing, increasing nearly tenfold from 2020 to 2023, and topping \$65 million in just the first *half* of 2024.<sup>3</sup> Since the vast majority of frauds are not reported, this likely reflects only a fraction of the actual harm.<sup>4</sup>

### Reported BTM fraud losses by year

January 2020 - June 2024



These figures are estimates based on keyword analysis of the narratives provided in reports to the FTC's Consumer Sentinel Network that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a BTM was used. The estimated number of reports by year are as follows: 902 (2020), 1,981 (2021), 3,698 (2022), 4,863 (2023), and 2,968 (through June 2024).

Cryptocurrency surged as a major payment method for scams in recent years, along with the massive growth in crypto payments on fake investment opportunities.<sup>5</sup> But now crypto is a top payment method for many other scams, too.<sup>6</sup> Widespread access to BTMs has helped make this possible. Reports of losses using BTMs are overwhelmingly about government impersonation, business impersonation, and tech support scams.<sup>7</sup> And when people used BTMs, their reported losses are exceptionally high. In the first six months of 2024, the median loss people reported was \$10,000.<sup>8</sup>

In the first half of the year, people 60 and over were more than three times as likely as younger adults to report a loss using a BTM.<sup>9</sup> In fact, more than two of every three dollars reported lost to fraud using these machines was lost by an older adult.<sup>10</sup>

Scams that use BTMs work in lots of different ways. Many start with a call or message about supposed suspicious activity or unauthorized charges on an account.<sup>11</sup> Others get your attention with a fake security warning on your computer, often impersonating a company like Microsoft or Apple. These things are hard

to ignore, and that's the point. From there, the story quickly escalates. They might say all your money is at risk, or your information has been linked to money laundering or even drug smuggling. The scammer may get a fake government agent on the line – maybe even claiming to be from the “FTC” – to up the ante.

So where do BTMs fit into the story? Scammers claim that depositing cash into these machines will protect your money or fix the fake problem they've concocted. They've even called BTMs “safety lockers.” They direct you to

go to your bank to take out cash. Next, they send you to a nearby BTM location – often a specific one – to deposit the cash you just took out of your bank account.<sup>12</sup> They text you a QR code to scan at the machine, and once you do, the cash you deposit goes right into the scammer’s wallet.

So how can you spot and steer clear of these scams?

- Never click on links or respond directly to unexpected calls, messages, or computer pop-ups. If you think it could be legit, contact the company or agency, but look up their number or website yourself. Don't use the one the caller or message gave you.
- Slow down. Scammers want to rush you, so stop and check it out. Before you do anything else, talk with someone you trust.
- Never withdraw cash in response to an unexpected call or message. Only scammers will tell you to do that.
- Don't believe anyone who says you need to use a Bitcoin ATM, buy gift cards, or move money to protect it or fix a problem. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

To spot and avoid scams visit [ftc.gov/scams](https://ftc.gov/scams). Report scams to the FTC at [ReportFraud.ftc.gov](https://ReportFraud.ftc.gov).

1 While machines that allow consumers to buy cryptocurrency are commonly referred to as Bitcoin ATMs or BTMs, these machines often handle – and scams can take place in – other cryptocurrencies in addition to Bitcoin.

2 BTM installations self-reported by operators to an industry website increased from about 4,250 in January 2020 to about 32,000 in June 2024. See trend chart available at <https://coinatmradar.com/charts/growth/united-states/>.

3 These and other figures throughout this Spotlight are estimates based on keyword analysis of the narratives provided in reports that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a BTM was used.

4 See Anderson, K. B., *To Whom Do Victims of Mass-Market Consumer Fraud Complain?* at 1 (May 2021), available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3852323](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323) (study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity).

5 See FTC Consumer Protection Data Spotlight, *Reports Show Scammers Cashing in on Crypto Craze* (June 3, 2022), available at <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammerscashing-crypto-craze>.

6 In the first half of 2024, cryptocurrency was the top payment method in terms of aggregate reported losses on tech support scams and job scams, and the second most costly method after bank transfers on business impersonation scams, government impersonation scams, romance scams, and family and friend impersonation scams.

7 In the first half of 2024, about 86% of people who reported a fraud loss using a BTM indicated that it was on a government impersonation, business impersonation, and/or tech support scam. This excludes reports categorized as unspecified.

8 In the first half of 2024, the median individual reported fraud loss when cryptocurrency was the reported payment method (including reports with and without BTM use) was \$5,400; the median individual reported loss to fraud generally was \$447.

9 This comparison of older and younger consumers' reporting rates is normalized based on the population size of each age group using the Census Bureau's 2018-2022 American Community Survey 5-Year Estimates. This excludes reports that did not include consumer age information.

10 In the first half of 2024, people 60 and over reported losing \$46 million using BTMs, or about 71% of the reported losses using these machines. During the same period, when a reported cryptocurrency fraud loss did *not* involve the use of a BTM, about 72% of the losses were reported by people 18 to 59. Most of these losses were to fake cryptocurrency investment opportunities. Percentage calculations exclude reports that did not include consumer age information.

11 Phone calls were the initial contact method in about 47% of these reports, followed by online ads or pop-ups (16%), and e-mails (9%). Reports indicating online ad or pop-up as the contact method typically described fake computer security alerts. People reported that security pop-ups and email messages included a phone number to call for help.

12 Reports show that scammers direct people to specific BTM locations and many consumers name the BTM operator in their reports. These details show a pattern that suggests scammers prefer some operators over others and that these preferences have changed over time. While the reports do not tell us why this might be, differences in fraud prevention measures taken by various operators likely play a role.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at [ReportFraud.ftc.gov](https://ReportFraud.ftc.gov). To explore Sentinel data, visit [FTC.gov/exploredata](https://FTC.gov/exploredata).

HOUSE INDUSTRY, BUSINESS AND LABOR COMMITTEE  
JONATHAN WARREY, CHAIRMAN  
JANUARY 22, 2025

TESTIMONY BY  
ELIN S. ALM  
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL  
RE: HOUSE BILL NO. 1447

Mr. Chairman and members of the Industry, Business, and Labor Committee. I am Elin Alm, and I serve as the Director of the Attorney General's Consumer Protection and Antitrust Division. I appear on behalf of the Attorney General in support of House Bill No. 1447 and to provide some background on the significance of House Bill No. 1447 for consumer protection.

Over the last few years, the Attorney General's Office has noticed a substantial increase in reports of scammers employing the use of virtual currency kiosks. Data from the Federal Trade commission shows that fraud losses at virtual currency kiosk have skyrocketed and increased nearly tenfold between 2020 and 2023. Most of the scams employing the virtual currency kiosks are government impersonation, business impersonation, or tech support scams. Numerous North Dakota residents have reported loss of significant amounts of money to scammers instructing them to deposit money into the virtual currency kiosk to safeguard their money or to make supposedly required payments. To illustrate how the virtual currency kiosk is used in scams, I will provide a few real examples of the reports we received in 2024, where the reported losses exceeded half a million dollars:

- On May 2, 2024, an elderly Bismarck woman received a Microsoft pop-up on her computer. She called the number and talked to "Austin" who represented he was with fraud protection and that \$30,000 had been taken from her account. The woman was told that her bank and the Federal Reserve were also involved. She was instructed to remove all her money from her bank and deposit the money into a "Federal ATM machine." She made two deposits (\$20,000 & \$12,000) at the virtual currency kiosk at a gas station. When she was prevented from sending more through that machine, she was instructed to make an additional two deposits (\$15,000 & \$25,000) at a virtual currency kiosk at a grocery store. The woman later went to her bank and learned she had been victim of a scam and had lost the \$72,000 that she deposited in the virtual currency kiosk.

- In August of 2024, a Bismarck woman was experiencing issues with her iMac computer and searched for a phone number for Apple support on the internet. She found a number represented to be for Apple Support. When she called the number, she was told her devices were compromised and there were charges on her accounts. The scammer gave her what he represented to be a claim number with the FTC and proceeded to help the woman reach out to what the scammer called her banks' "headquarters". The person at the banks' "headquarters" told the woman she needed to start a virtual account, take cash out of her bank, and deposit it into a "federal public machine" so the money can be traced federally to know she is attempting to fix the supposed problem. She then proceeded to put \$10,000 into a virtual currency kiosk as instructed, thereby transferring the \$10,000 to the scammer.
- In September of 2024, a 41-year-old Bismarck woman received a phone call from an individual who identified himself as being with the Burleigh County Sheriff's Office. The scammer claimed that the woman had failed to appear on a federal warrant and was in contempt of court. She was instructed to send \$5,500 through a virtual currency kiosk to pay the fine and clear her name. Consequently, she withdrew \$5,500 from her bank and deposited the money into a virtual currency kiosk at a grocery store in Bismarck, thereby losing the money to the scammer.
- In October of 2024, a 63-year-old Dickinson woman fell victim to a government imposter scam when she was told that because of Identity Theft, she was going to be arrested for money laundering. She withdrew \$13,000 from her bank account and was told to deposit the money in a virtual currency kiosk for "safe keeping," when in fact she was sending it to the scammer. She was then instructed to pull another \$70,000 from her retirement account. Luckily, her employer intervened before she lost additional funds.
- In October of 2024, a 62-year-old Carrington man reported that he was a victim of a Pig Butchering scam. The man had entered an online relationship with who he believed was a female. The female subject had recommended that he begin investing in Bitcoin, to which he agreed. During this scam, the man went to multiple virtual currency kiosks and purchased approximately \$354,500.00 in Bitcoin, all of which were transferred to the scammer and lost.

So far in January of 2025, three North Dakota residents have already reported losses in the combined amount of \$34,000 to scams that involved the use of virtual currency kiosks. Two reports involved Jury Duty Scams with losses of \$9,000 and \$9,500. The third report involved an Account Compromise Scam where the consumer lost \$15,500 transferred to the scammer through a virtual currency kiosk after she was falsely led to believe that an



error had been made resulting in her receiving a \$19,999 refund on a fraudulent charge when she was only entitled to a \$199 refund.

Virtual currency kiosks are a particularly advantageous tool for scammers because the transactions are immediate and cannot be called back like a wire transaction, cancelled like a gift card, or intercepted like a package. The virtual currency kiosks provide an instant and easy one-step method to steal money from consumers, because it eliminates the opportunity for victims to stop or reverse the transaction when they realize they have been scammed. Scammers are also able to take advantage of consumers unfamiliarity with virtual currency and the purpose and functionality of the virtual currency kiosks.

House Bill No. 1447, if enacted, can help protect every North Dakota resident from losing money to a scam. Scammers are becoming more sophisticated and manipulative, and scams can ensnare even the most intelligent and financially savvy person. Scammers are criminals whose playbook includes the employment of a psychological warfare to steal consumers hard earned money. Many scams start with a call or message about supposed suspicious activity or unauthorized charges on an account or a fake security warning on a computer, and such messages are hard to ignore.

It's important to keep in mind that under the right circumstances, anyone can become a victim of a scam. We know the prevalence of scams is much higher than what's reported. Because there is a stigma that remains around scams - the misconception that victims are naive, unintelligent, uneducated, or experiencing cognitive decline - victims feel helpless, ashamed, alone, and are unwilling to report incidents of fraud. We often hear from scam victims, who are willing to report, that they are ashamed and embarrassed because they feel they should have known better and cannot believe that this happened to them. It may be easy with the benefit of hindsight to see the signs of a scam. However, when you are in a situation where you are contacted by someone with apparent authority, with threats of serious consequences unless you take swift action as instructed to protect yourself, your family, or your money, it does not appear or feel like a scam.

While the existence of scams is a global problem that is hard to combat, there are measures that can be put in place to at least make it harder for scammers to perpetrate and profit from scams against North Dakota residents. House Bill No. 1447 represents such a measure through its required display of warnings and disclosures and the daily limit on transactions. Therefore, the Attorney General supports a "Do Pass" recommendation on House Bill No 1447. Thank you for your time and consideration. I would be happy to try and answer any questions.



**ORAL TESTIMONY SUBMITTED TO THE NORTH DAKOTA  
HOUSE INDUSTRY, BUSINESS AND LABOR COMMITTEE  
Kevin Lolli, Assistant General Counsel and Consumer Protection Officer  
January 22, 2025**

Chair Warrey, Vice-Chair Ostlie, and honorable members of the House Industry, Business and Labor Committee, thank you for the opportunity to provide testimony today regarding HB 1477.

CoinFlip opposes certain language in HB 1477 relating to the proposed regulation of virtual currency kiosks. However, CoinFlip does support certain proposed regulatory measures that would further consumer protection including but not limited to licensure, mandatory disclosures, compliance program requirements, and technology requirements. We appreciate the opportunity to offer additional consumer protection-focused recommendations that we know to be highly effective in preventing fraudulent transactions at virtual currency kiosks and look forward to continuing to work with the State of North Dakota to protect consumers.

**Company Background**

CoinFlip is a Chicago-based, global digital currency platform, focused on providing consumers a simple and secure way to buy and sell virtual currency. Founded in 2015, CoinFlip is one of the world's largest operators of virtual currency kiosks, with more than 5,000 locations across the United States and in nine countries around the world, employing more than 200 people.

CoinFlip's kiosks make buying and selling major cryptocurrencies accessible and secure for consumers who wish to purchase their virtual currency using cash. CoinFlip has operated in the State of North Dakota since 2018 and was originally granted a North Dakota money transmitter license by the North Dakota Department of Financial Institutions on October 10, 2023. Additionally, CoinFlip is a money service business ("MSB") registered with the Financial Crimes Enforcement Network. As an MSB, CoinFlip is subject to the Bank Secrecy Act ("BSA"), the United States PATRIOT Act, and their implementing rules and regulations.

CoinFlip embraces licensing regimes as an effective means to create baseline requirements for operations, as well as effective oversight. CoinFlip holds approximately 26 money transmitter licenses with numerous additional applications currently pending. CoinFlip has moved to obtain these licenses, even in states where there is no current licensing requirement.

**Advancing Consumer Protection**

As a company, one of CoinFlip's key business priorities is consumer protection. We won't succeed unless our customers believe we provide them with a safe and secure platform from which to transact virtual currency. CoinFlip's compliance and consumer protection efforts are currently

overseen by its Chief Legal Officer, General Counsel, BSA Officer, and Consumer Protection Officer. To effectively manage the risks associated with its operations, CoinFlip implements both traditional consumer protection efforts such as clear disclosures and warnings, as well as state-of-the-art technology to detect and fight fraudulent transactions.

When transacting with a CoinFlip kiosk, customers are warned numerous times regarding scam-related activity prior to initiating *every* transaction. The customer must attest that they were not sent to the kiosk by a third-party to make a payment; that they are transacting with a digital wallet they own and control; and that they understand all transactions are final and irreversible. This screen is customizable and is updated regularly with warnings about common scams to alert customers and help fight fraud. We also provide clear disclosures on fees and provide customers with a receipt of their transaction via email or text.

Additionally, CoinFlip has 24/7 live customer service and lists its number both on the physical kiosk as well as its transaction screens. Customers are instructed to call CoinFlip in the event a third-party sent them to transact at the kiosk. CoinFlip customer service representatives receive training at least twice annually on AML/BSA requirements and how to be the first line of defense in compliance efforts. As a result of these efforts, CoinFlip's customer support team halted more than 300 potential scams in a four-month period by speaking with the customer who phoned our support team after reading the customer warnings at our kiosk.

CoinFlip also implements state-of-the-art blockchain analytics and compliance tools to block fraudulent transactions and investigate suspicious activity. CoinFlip has automatically blocked more than 1,000 transactions using blockchain analytics in a year's period. In addition to blocking transactions, CoinFlip permanently blacklists digital wallet addresses to prevent those high-risk digital wallets from ever being used at a CoinFlip kiosk again.

### **HB 1447**

Unfortunately, HB 1447 relies on policy recommendations that create a false sense of consumer protection. The proposed transaction limits in the bill do not adequately consider federal reporting requirements. Under federal law, CoinFlip is required to file a Suspicious Activity Report ("SAR") for any suspected suspicious transactions above \$2,000 and a Currency Transaction Report ("CTR") for transactions above \$10,000. This information is placed in a repository for law enforcement to quickly and accurately conduct investigations. North Dakota's proposed \$1,000 transaction limit encourages stacking transactions across multiple kiosk operators, and limits companies' Anti-Money Laundering efforts. Further, the limit will result in less information available to law enforcement as kiosk operators will no longer file any SAR or CTR.

The addition of transaction fee caps does not prevent customer fraud and in combination with transaction limits, inadvertently creates incentives for less transparency and less use of expensive compliance tools which keep consumers safe. Unlike online exchanges, virtual currency kiosk operators have additional operational costs such as device hardware and maintenance, rent payments to local small business hosts, armored car service costs, customer service, and blockchain analytics. The proposed North Dakota fee limits do not take into consideration these unique operational costs and are a de facto ban of virtual currency kiosks in North Dakota.

Lastly, the refund provisions found in HB 1447 are unprecedented for money service businesses. No responsible money service business wants to profit off possible fraudulent transactions; however, requiring a refund for the entire transaction requires virtual currency kiosk operators to insure every transaction and encourages fraudsters to defraud kiosk operators.

### **Proposed Consumer Protection Policies**

CoinFlip believes smart regulation is good for business. We believe that a regulatory framework is necessary to protect consumers and encourage innovation in the industry; however, transaction limits, fee limits, and refund provisions as currently proposed in HB 1447 are a de facto ban on operating in the State of North Dakota and do not take into consideration federal reporting requirements. Instead, we developed the following best practices that would further enhance consumer protections and support their inclusion in any legislation:

- **Require licensure with the state.** CoinFlip believes a money transmitter license should be required for all virtual currency kiosk operators, allowing for state oversight and periodic audits to determine the adequacy of compliance, finance, and cybersecurity programs.
- **Require robust compliance programs.** Kiosk operators should be required to directly employ a qualified, in-house, Chief Compliance Officer and compliance team, that does not have a large ownership interest in the company. At CoinFlip, we take compliance seriously: our Chief Compliance Officer is a former federal prosecutor, and our general counsel is a former Illinois Assistant Attorney General.
- **Require clear, highly visible warnings and fee disclosures.** We agree with the proposed legislation regarding the requirement of clear disclosures regarding all fees and terms of service. We also believe highly visible fraud warnings should be required to be displayed and acknowledged by the customer prior to the initiation and completion of any transaction.
- **Require blockchain analytics.** The use of blockchain analytics technology should be required to fight fraud by automatically blocking customer transactions to high-risk digital wallets.
- **Require live customer service.** Customer service is the first line of defense for consumer protection. We believe every virtual currency kiosk operator should be required to provide trained, live customer service at minimum during business hours.

CoinFlip shares your goals of consumer protection. Although blockchain technology and virtual currency kiosks are new, the fraud we see reported is all too familiar. Whether it's phone, email, text or an online pop-up, scammers repackage the same old tactics and utilize whatever methods they have at hand – Venmo, PayPal, Zelle, Gift Cards, MoneyGram or virtual currency kiosks – to dupe people out of their money.

The best defense for consumers is to be well-informed and well-alerted at the point of transaction. The best defense for companies is to have the right tools in place to help identify and fight fraud and help law enforcement catch the bad actors.

## **Conclusion**

In conclusion, we believe that a regulatory framework is necessary to protect consumers and encourage innovation and we look forward to working with the North Dakota House to improve HB 1447 to achieve the right balance to protect North Dakota consumers and ensure continued access for lawful virtual currency transactions.

Thank you for your time and consideration.

Sincerely,

/s/ Kevin P. Lolli

Kevin Lolli  
*Assistant General Counsel*



North Dakota House Industry, Business and  
Labor Committee  
Room JW327C  
North Dakota State Capitol  
Bismark, ND 58505

**BITCOIN DEPOT**

2870 Peachtree Rd. NW, #327  
Atlanta, GA 30305  
[www.bitcoindepot.com](http://www.bitcoindepot.com)  
PH: (678) 961-0059  
FAX: (470) 430-3609

Thank you Chairman and Members of the Industry, Business and Labor Committee, I am Ethan McClelland, the Director of Government Relations at Bitcoin Depot, the largest operator of cryptocurrency kiosks in the world. Thank you for your time and affording me the opportunity to speak about our perspective on HB 1447.

Our business model is that we place our kiosks into retail centers such as gas stations and convenience stores; renting that space from small businesses. A customer inserts cash into the kiosk following a thorough review of their identity and checking against suspicious activity, is able to purchase bitcoin and transfer it to their digital wallet, where they are sole owners of that bitcoin.

Our kiosks are placed in a wide variety of neighborhoods in North Dakota. Our customers include the underbanked and unbanked, as well as those who work in cash-heavy businesses such as trades, construction, or service industries and wish to participate in the cryptocurrency market. They value the physical presence of kiosks versus utilizing an online exchange, as well as the ability to outright own cryptocurrency, rather than exposing themselves to the risks associated with the collapse of an exchange, as we saw in the case of FTX. Individuals who have used our services have self-designated that the primary purpose for purchasing bitcoin is sending funds to family members abroad, online payments and purchases, remittances and money transfers, and investment or store of value.

There are many provisions in HB 1447 that we support and in nearly every case, are already doing such as, requiring kiosk companies who wish to do business in North Dakota to follow a rigorous licensing program, requiring clear disclosures ranging from the risks involved in the cryptocurrency market to clearly displayed anti-fraud warnings, as well as building a mature compliance program, to include the use of third party blockchain analytics.

However, we have serious concerns with provisions in HB 1447 that would effectively prevent kiosk companies from doing business in North Dakota because of the overly aggressive nature of the limits on daily transactions, as well as the unreasonably low fee cap provision. In essence, HB 1447 in its current form would drive our business from North Dakota.

Placing permanent or long-term transaction limits have unintended consequences including leading criminals to skirt federal reporting requirements. For example, the Financial Crimes Enforcement Network, or FinCen, requires companies to submit Suspicious Activity Reports on potential scams or questionable transactions for any transaction flagged that is above \$2000. They then transmit this information to law enforcement to combat local scam activity. Fincen lacks the resources to process reports below \$2000 and does not allow SAR filings below that threshold. In essence, a \$1000 transaction limit would deny North Dakota law enforcement valuable data on how to combat scams. Furthermore, transaction limits encourage both good and bad actors to spread transactions across multiple kiosk operators, further hiding scam and illicit activity. And, legitimate customers choosing to use alternate banking methods such as



---

kiosks should not suffer additional “taxation” in the form of “kiosk-shopping” to multiple locations to complete necessary transactions.

Operating a cryptocurrency kiosk has unique costs, including purchasing, installing, and maintaining the kiosk equipment. There are also recurring costs, including rent to small businesses hosting a kiosk, insurance, legal fees, bank fees, blockchain access fees, cash management, armored vehicles, monitoring and surveillance, BSA / AML / OFAC compliance, cybersecurity, fraud detection, and live customer support. Exchanges that custody funds do not have the hardware costs that kiosk operators maintain. Other financial service companies that hold funds can assess fees in multiple touchpoints during the relationship; we cannot. And bad kiosk operators who may charge lower fees do not maintain strong compliance and consumer safeguards. The current proposed fee cap of 3% would be the lowest in the country. What we have seen in states with low transaction limits such as California is legitimate “good” operators such as ourselves leave the state because of a lack of profit, while “bad” operators remain, skirting the already thin enforcement resources of the Department, meaning scam activity remains.

We are proud of the company we have built and the steps we have taken to balance innovation with security and the safety of our customers. We are willing to work with the committee to continue to hone HB 1447 into legislation we can support that fosters innovation, protects consumers and allows business to thrive. Unfortunately, in its current form, we feel that HB 1447 regrettably falls short of that goal. In order to allow that conversation to continue, I would ask that the committee vote to not send it to the full house at this time. We appreciate your time, and welcome any questions and the opportunity to continue the conversation.





January 21<sup>st</sup>, 2025

**Mr. Chairman and members of the House Industry, Business, and Labor Committee:**

My name is Jacob Rued. I am Minot native and currently reside in rural Cass County.

For over the past decade, I have had the opportunity to serve our state in various law enforcement and private sector fraud prevention roles. I have proudly served our communities as a Cass County Deputy Sheriff, Fargo Police Officer, and Fargo Police Financial Crimes Detective. I currently work as a Fraud Investigator for the Minot-based community bank, First Western Bank. I hold certifications as a Certified Fraud Examiner by the Association of Certified Fraud Examiners and as a Certified Anti-Money Laundering and Fraud Professional by the American Bankers Association.

I write this testimony to you in fervent support of HB 1447 on behalf of myself, First Western Bank, and Independent Community Banks of North Dakota.

Unfortunately, my job must exist because of criminals who steal and defraud millions of dollars from North Dakotans using crypto kiosks, which scammers often deceptively refer to as "Federal Safety Lockers". In many cases I have investigated, our community members are indoctrinated, through fear, to withdraw their life savings in cash and deliver them to a crypto kiosk in their community or neighboring community. Once deposited, their funds are gone, unrecoverable, certainly not in a "safety locker".

Our victims, often but not exclusively seniors, are rarely versed in understanding cryptocurrency or involved in legitimate investment with it. Their engagement with a crypto kiosk marks the first, last, and likely only cryptocurrency transaction they will ever complete. Their trust in the kiosk often based on the manipulated idea because the kiosk is "real" and physically present in their community, must mean any associated business is vetted like a traditional ATM. *Why or how else would it be here?*

I believe HB 1447 strikes a reasonable balance in continuing to allow North Dakotans to engage with the plethora of legitimate, online crypto exchanges they may make deposits to via check, wire, and ACH while limiting a vulnerable population's exposure to a type of currency they are not familiar with. Furthermore, I applaud HB 1447's requirement of receipted disclosures, operator fraud prevention requirements, fraud reimbursement criteria, daily transaction limits, and a cap of fees.

In closing – I offer you 2 further points to assist in your evaluation and decisioning on this bill.

1. First Western Bank operates in both Minnesota and North Dakota. In August of 2024, Minnesota enacted legislation nearly identical to HB 1447. The following is a contrast between 2 of my cases in these states:
  - a. *North Dakota Resident* – young, newlywed couple (20s YOA). Husband is called and extorted to believe there is a warrant for his arrest. Husband withdraws \$15K from their bank account. Deposits all \$15K cash at a local crypto kiosk believing this will pay his government fines and prevent him from going to jail. Husband later realizes he was scammed. The couple is at 100% loss. The \$15K was a relatively considerable sum and intended to be used as a down payment on a house. Victim has otherwise never used crypto currency.
  - b. *Minnesota Resident* – elderly, retired couple. Husband is called and convinced someone in his bank is stealing his money. The "FBI" needs him to withdraw all his funds and deposit them in a "safety locker". Husband withdraws all \$50K from his savings and takes all \$50K to a nearby kiosk at a gas station. Husband feeds \$2K to the ATM but is stopped because of MN law limiting his deposit to \$2K. Husband realizes he's been scammed. Returns \$48K to the bank with only a \$2K loss. Victim has otherwise never used crypto currency.
2. First Western Bank is a \$2Bn asset institution, with over 350 employees, operating in 3 states. Consider this context in the following example:
  - a. An elderly victim is deceived to believe they are investing in a lucrative international business. Investments in these stocks/securities are made via crypto currency, partially by kiosk. The victim eventually learns the business does not exist and the \$200K+ funds he invested, and recruited other members in his community to invest, are lost. The crypto deposits are traced to a crypto wallet holding over \$2Bn worth of Bitcoin at that time's market value. At current market value, this would be approximately \$4Bn USD of Bitcoin.

I can't tell you who controls that \$4Bn, because the nature of Bitcoin doesn't make that possible, but I know whoever or whatever organization does control it, certainly is not using it for anything that will benefit our state or our way of life.





## **Written Testimony in Support of HB 1447: Virtual Currency Kiosk Fraud Prevention**

Chairman Warrey and Members of the Committee,

For the record, my name is John Alexander, and I am here today on behalf of the Dakota Credit Union Association (DakCU), representing Both State chartered and federally chartered credit unions across North Dakota. We support the enactment of House Bill 1447, which introduces critical protections for consumers using virtual currency kiosks.

The conversation around cryptocurrency scams often focuses on elderly victims, but what we don't talk about enough is how these scams are devastating young adults—college students, single parents, and young professionals—many of whom are already struggling to make ends meet.

At credit unions, we see the real impact of financial fraud. We hear from members who have lost everything in a matter of minutes. One such case involved a 22-year-old college student from Fargo who, after receiving a panicked call from someone claiming to be from her bank's fraud department, was told her checking account had been compromised. The "representative" convinced her to withdraw \$1,500 in cash—the money she had saved for next month's rent—and deposit it into a nearby crypto ATM to "secure" her funds". She scanned a QR code the scammer sent her, and within seconds, her money was gone. She was left with no way to pay rent, no emergency funds, and nowhere to turn.

In another case, a young father from Bismarck, already struggling to keep up with daycare costs, was targeted by a fake tech support scam. His laptop froze, flashing an alert that his bank account had been hacked and urging him to "secure" his funds by transferring them through a Bitcoin ATM. He rushed to withdraw \$2,000—everything he had in savings—and deposited it into a machine at a gas station. The moment he pressed "confirm," the scammer disconnected, and his funds were unrecoverable.

These aren't just statistics. These are real people—young workers, students, and parents—who are one scam away from financial ruin. Unlike older adults who may have built-up savings, younger victims often don't have a financial cushion to fall back on. For them, a \$1,500 scam means eviction, car repossession, or being unable to afford groceries for the month.

HB 1447 addresses these threats by requiring virtual currency kiosk operators to implement fraud prevention measures, provide clear disclosures, and enforce daily transaction limits. Credit unions strongly support these efforts because, without these protections, these machines will



continue to be easy targets for fraudsters, preying on young consumers who often don't realize that crypto transactions are irreversible.

Unlike traditional ATMs, which are federally regulated and connected to consumer protections through banks and credit unions, crypto ATMs operate with little oversight. Many users don't even realize they are not protected. Scammers exploit this lack of regulation, directing victims to these machines because they know the transactions are instant and cannot be undone. By the time the victim realizes they've been tricked, the scammer has already moved the funds through multiple wallets, making recovery impossible.

HB 1447 helps level the playing field. By ensuring kiosk operators adhere to basic fraud prevention standards, the bill makes it harder for scammers to use these machines as tools for financial destruction.

Young North Dakotans should not have to live in fear that one wrong decision could cost them their entire financial future.

Thank you, Mr. Chairman and members of the Committee, for considering this important legislation. I am happy to answer any questions you may have.

John Alexander  
Dakota Credit Union Association  
Director of Legislative & Regulatory Affairs

A handwritten signature in black ink, appearing to read "John Alexander". The signature is fluid and cursive, with a stylized "J" and "A".

# 2025 HOUSE STANDING COMMITTEE MINUTES

## Industry, Business and Labor Committee Room JW327C, State Capitol

HB 1447  
2/12/2025

A BILL for an Act to create and enact a new chapter to title 54 of the North Dakota Century Code, relating to the advanced technology review committee, advanced technology grant program, and advanced technology grant fund; to provide for a transfer; and to provide an appropriation.

3:37 p.m. Vice Chairman Ostlie opened the meeting.

Members Present: Chairman Warrey, Vice Chairman Ostlie, Vice Chairman Johnson, Representatives Brown, Finley-DeVille, Grindberg, Kasper, Koppelman, D. Ruby, Schatz, Schauer, Vollmer. Member Absent: Representative Bahl.

Members Absent: Representatives Bahl, Christy.

### Discussion Topics:

- Daily limits
- 72 hours
- \$2000 up to 5 transactions per month
- 2 factor authentication

3:37 p.m. Representative Koppelman proposed Amendment LC # 25.1011.01002, testimony #37577.

3:42 p.m. Representative Koppelman moved Adopt Amendment LC # 25.1011.01002, #37577.

3:42 p.m. Representative Schauer seconded the motion.

Voice vote.

Motion passed.

3:44 p.m. Representative Koppelman moved Do Pass as amended.

3:44 p.m. Representative Johnson seconded the motion.

Representatives	Vote
Representative Jonathan Warrey	Y
Representative Mitch Ostlie	Y
Representative Landon Bahl	AB
Representative Collette Brown	Y
Representative Josh Christy	AB
Representative Lisa Finley-DeVille	Y

Representative Karen Grindberg	Y
Representative Jorin Johnson	Y
Representative Jim Kasper	Y
Representative Ben Koppelman	Y
Representative Dan Ruby	Y
Representative Mike Schatz	Y
Representative Austin Schauer	Y
Representative Daniel R. Vollmer	Y

Motion passed 12-0-2.

3:47 p.m. Representative Koppelman will carry the bill.

3:47 p.m. Vice Chairman Ostlie adjourned the meeting.

*Diane Lillis, Committee Clerk*



Sixty-ninth  
Legislative Assembly  
of North Dakota

**PROPOSED AMENDMENTS TO**

**HOUSE BILL NO. 1447**

Introduced by

Representatives Swiontek, Christy, Hanson, Heinert, Schauer, J. Olson, Richter

Senators Hogan, Klein, Lee, Rummel, Sickler

2-12-25  
JB 1 of 16

1 A BILL ~~for an Act to create and enact a new chapter to title 6 of the North Dakota Century Code,~~  
2 ~~relating to virtual currency kiosks.~~for an Act to create and enact sections 13-09.1-50,  
3 13-09.1-51, 13-09.1-52, 13-09.1-53, and 13-09.1-54 of the North Dakota Century Code, relating  
4 to virtual-currency kiosks; and to amend and reenact section 13-09.1-44 of the North Dakota  
5 Century Code, relating to virtual-currency kiosks.

6 **BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

7 ~~SECTION 1. A new chapter to title 6 of the North Dakota Century Code is created and~~  
8 ~~enacted as follows:~~

9 ~~Definitions.~~

10 ~~In this chapter unless context requires:~~

11 ~~1. "Blockchain analytics" means the analysis of data from blockchains or public~~  
12 ~~distributed ledgers, including associated transaction information.~~

13 ~~2. "Blockchain analytics software" means a software service that uses blockchain~~  
14 ~~analytics data to provide risk-specific information about virtual currency wallet~~  
15 ~~addresses.~~

16 ~~3. "Commissioner" means the commissioner of financial institutions.~~

17 ~~4. "New customer" means an individual who has never previously transacted with the~~  
18 ~~virtual currency kiosk operator and for the first thirty days after the first financial~~  
19 ~~transaction with the virtual currency kiosk operator.~~

Jan 2016

- 1 — ~~5. "Transaction hash" means a unique identifier made up of a string of characters that act~~  
2 ~~as a record and provide proof the transaction was verified and added to the~~  
3 ~~blockchain.~~
- 4 — ~~6. "Virtual currency address" means an alphanumeric identifier associated with a virtual~~  
5 ~~currency wallet identifying the location to which a virtual currency transaction can be~~  
6 ~~sent.~~
- 7 — ~~7. "Virtual currency kiosk" means an electronic terminal acting as a mechanical agent of~~  
8 ~~the virtual currency kiosk operator to enable the virtual currency kiosk operator to~~  
9 ~~facilitate the exchange of virtual currency for money, bank credit, or other virtual~~  
10 ~~currency, including by:~~
  - 11 — ~~a. Connecting directly to a separate virtual currency exchange that performs the~~  
12 ~~actual virtual currency transmission; or~~
  - 13 — ~~b. Drawing upon the virtual currency in the possession of the electronic terminal's~~  
14 ~~operator.~~
- 15 — ~~8. "Virtual currency kiosk operator" means a person that engages in virtual currency~~  
16 ~~business activity via a money transmission kiosk located in this state or a person that~~  
17 ~~owns, operates, or manages a money transmission kiosk located in this state through~~  
18 ~~which virtual currency business activity is offered.~~
- 19 — ~~9. "Virtual currency kiosk transaction" means a transaction conducted or performed, in~~  
20 ~~whole or in part, by electronic means via a virtual currency kiosk. Virtual currency~~  
21 ~~kiosk transaction also means a transaction made at a virtual currency kiosk to~~  
22 ~~purchase virtual currency with fiat currency or to sell virtual currency for fiat currency.~~
- 23 — ~~10. "Virtual currency wallet" means a software application or other mechanism providing a~~  
24 ~~means to hold, store, or transfer virtual currency.~~
- 25 — **Virtual currency kiosks.**
  - 26 — ~~1. A kiosk operator may not engage in virtual currency business activity or hold itself out~~  
27 ~~as being able to engage in virtual currency business activity with or on behalf of~~  
28 ~~another person unless the kiosk operator is licensed in this state as a money~~  
29 ~~transmitter.~~
  - 30 — ~~2. A virtual currency kiosk operator shall comply with all requirements of a money~~  
31 ~~transmitter under chapter 13-09.1.~~



83 3d/16

- ~~3. A virtual currency kiosk operator may not locate, or allow a third party to locate, a virtual currency kiosk in this state unless the virtual currency kiosk:~~
  - ~~a. Is placed a commercially accessible area;~~
  - ~~b. Is accessible to users with sufficient space to account for mobility limitations of users;~~
  - ~~c. Is subject to security features, including sufficient lighting and surveillance; and~~
  - ~~d. Complies with any additional restrictions or requirements as required by the commissioner.~~
- ~~4. Each virtual currency kiosk operator shall submit a quarterly report of the location of each virtual currency kiosk located within the state to the commissioner within forty-five days of the end of the calendar quarter. The location report must include:~~
  - ~~a. The company legal name;~~
  - ~~b. Any fictitious or trade name;~~
  - ~~c. The physical address;~~
  - ~~d. The start date of operation of the virtual currency kiosk at the location;~~
  - ~~e. The end date of operation of the virtual currency kiosk at the location, if applicable; and~~
  - ~~f. The virtual currency addresses associated with the virtual currency kiosk.~~
- ~~**Disclosures.**~~
  - ~~1. A virtual currency kiosk operator shall disclose in a clear, conspicuous, and easily readable manner in the chosen language of the customer, all relevant terms and conditions generally associated with the products, services, and activities of the virtual currency kiosk operator and virtual currency.~~
  - ~~2. The virtual currency kiosk operator must receive acknowledgment of receipt of all disclosures required under this section via confirmation of consent.~~
  - ~~3. Each virtual currency kiosk must include a warning written prominently and in bold type, stating substantially the following form:~~
    - ~~a. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:~~
      - ~~(1) Claims of a frozen bank account or credit card.~~

JB 4/08/16

- 1 ~~(2) Fraudulent bank transactions.~~
- 2 ~~(3) Claims of identity theft or job offerings in exchange for payments.~~
- 3 ~~(4) Requests for payments to government agencies or companies.~~
- 4 ~~(5) Requests for disaster relief donations or loans.~~
- 5 ~~(6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for~~
- 6 ~~vehicles.~~
- 7 ~~(7) Prompts to click on desktop popups, such as virus warnings or~~
- 8 ~~communication from alleged familiar merchants.~~
- 9 ~~(8) Communication from someone impersonating a representative of your bank~~
- 10 ~~or a law enforcement officer.~~
- 11 ~~(9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL YOUR LOCAL LAW~~
- 12 ~~ENFORCEMENT BEFORE ANY TRANSACTION.~~
- 13 ~~b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE~~
- 14 ~~RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS VIRTUAL~~
- 15 ~~CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE RISKS AND~~
- 16 ~~WISH TO CONTINUE WITH CONDUCTING MY VIRTUAL CURRENCY KIOSK~~
- 17 ~~TRANSACTION. PROTECT YOURSELF FROM FRAUD. NEVER SEND MONEY~~
- 18 ~~TO SOMEONE YOU DON'T KNOW.~~
- 19 ~~4. The commissioner shall require the disclosure of material risks associated with virtual~~
- 20 ~~currency and virtual currency transactions, including:~~
- 21 ~~a. The transaction may not be reversed;~~
- 22 ~~b. The virtual currency kiosk operator's liability for unauthorized virtual currency~~
- 23 ~~transactions;~~
- 24 ~~c. The virtual currency kiosk customer's liability for unauthorized currency~~
- 25 ~~transactions;~~
- 26 ~~d. Virtual currency is not legal tender, backed or insured by the government, and~~
- 27 ~~accounts and value balances are not subject to federal deposit insurance~~
- 28 ~~corporation, national credit union administration, or securities investor protection~~
- 29 ~~corporation protections;~~



Jan 5 of 16

- 1 ~~e. Some virtual currency transactions are deemed to be made when recorded on a~~
- 2 ~~public ledger which may not be the date or time when the individual initiates the~~
- 3 ~~transaction;~~
- 4 ~~f. Virtual currency's value may be derived from market participants' continued~~
- 5 ~~willingness to exchange fiat currency for virtual currency, which may result in the~~
- 6 ~~permanent and total loss of a particular virtual currency's value if the market for~~
- 7 ~~virtual currency disappears;~~
- 8 ~~g. An individual who accepts a virtual currency as payment today is not required to~~
- 9 ~~accept and might not accept virtual currency in the future;~~
- 10 ~~h. The volatility and unpredictability of the price of virtual currency relative to fiat~~
- 11 ~~currency may result in a significant loss over a short period;~~
- 12 ~~i. The nature of virtual currency means any technological difficulties experienced by~~
- 13 ~~virtual currency kiosk operators may prevent access to or use of an individual's~~
- 14 ~~virtual currency; and~~
- 15 ~~j. Any bond maintained by the virtual currency kiosk operator for the benefit of an~~
- 16 ~~individual may not cover all losses an individual incurs.~~
- 17 ~~5. The commissioner shall require disclosure of:-~~
- 18 ~~a. The amount of the transaction denominated in United States dollars as well as~~
- 19 ~~the applicable virtual currency;~~
- 20 ~~b. Any fees or expenses charged by the virtual currency kiosk operator;~~
- 21 ~~c. Any applicable exchange rates;~~
- 22 ~~d. A daily virtual currency transaction limit of no more than one thousand dollars;~~
- 23 ~~e. Notice of a change in the virtual currency kiosk operator's rules or policies;~~
- 24 ~~f. The name, address, and telephone number of the owner of the kiosk and the~~
- 25 ~~days, time, means by which a consumer can contact the owner for consumer~~
- 26 ~~assistance. Any relevant state and local law enforcement agency for reporting~~
- 27 ~~fraud must be displayed on or at the location of the virtual currency kiosk or on~~
- 28 ~~the first screen of the kiosk;~~
- 29 ~~g. Under what circumstances the virtual currency kiosk operator, without a court or~~
- 30 ~~government order, discloses a person's account information to third parties; and~~



- 1 ~~h. Other disclosures customarily given in connection with a virtual currency~~
- 2 ~~transaction.~~
- 3 ~~6. After the completion of each transaction, the virtual currency kiosk operator shall~~
- 4 ~~provide an individual with a physical receipt in the language chosen by the customer~~
- 5 ~~containing the following:~~
- 6 ~~a. The virtual currency kiosk operator's name and contact information, including a~~
- 7 ~~telephone number to answer questions and register complaints;~~
- 8 ~~b. Relevant state and local law enforcement or government agency for reporting~~
- 9 ~~fraud;~~
- 10 ~~c. The type, value, date, and precise time of the transaction, transaction hash, and~~
- 11 ~~each applicable virtual currency address;~~
- 12 ~~d. The name and contact information of the sender;~~
- 13 ~~e. The name and contact information of the designated recipient;~~
- 14 ~~f. All fees charged;~~
- 15 ~~g. The exchange rate of the virtual currency to United States dollars;~~
- 16 ~~h. A statement of the virtual currency kiosk operator's liability for nondelivery or~~
- 17 ~~delayed delivery;~~
- 18 ~~i. A statement of the virtual currency kiosk operator's refund policy; and~~
- 19 ~~j. Any additional information the commissioner may require.~~
- 20 ~~**Prevention of fraudulent activity.**~~
- 21 ~~1. A virtual currency kiosk operator shall use blockchain analytics software to assist in~~
- 22 ~~the detection and prevention of suspicious activity, including sending purchased virtual~~
- 23 ~~currency from a virtual currency kiosk operator to a virtual currency wallet known to be~~
- 24 ~~affiliated with fraudulent activity at the time of a transaction and identifying patterns~~
- 25 ~~that reflect money laundering or other illicit activity. The commissioner may request~~
- 26 ~~evidence from any virtual currency kiosk operator of use of blockchain analytics.~~
- 27 ~~2. A virtual currency kiosk operator shall take reasonable steps to detect and prevent~~
- 28 ~~fraud, including establishing and maintaining a written antifraud policy. The antifraud~~
- 29 ~~policy must include:~~
- 30 ~~a. The identification and assessment of fraud-related risk areas;~~
- 31 ~~b. Procedures and controls to protect against identified risks;~~



8370616

- 1 ~~c. Allocation of responsibility for monitoring risks; and~~
- 2 ~~d. Procedures for the periodic evaluation and revision of the antifraud procedures,~~
- 3 ~~controls, and monitoring mechanisms.~~
- 4 ~~3. Each virtual currency kiosk operator shall designate and employ a compliance officer~~
- 5 ~~with the following requirements:~~
- 6 ~~a. The individual must be qualified to coordinate and monitor compliance with this~~
- 7 ~~chapter and all other applicable federal and state laws and rules;~~
- 8 ~~b. The individual must be employed full time by the virtual currency kiosk operator;~~
- 9 ~~and~~
- 10 ~~c. The designated compliance officer may not be any individual who owns more~~
- 11 ~~than twenty percent of the virtual currency kiosk operator by whom the individual~~
- 12 ~~is employed.~~
- 13 ~~4. Compliance responsibilities required under federal and state laws and rules must be~~
- 14 ~~completed by full time employees of the virtual currency kiosk operator.~~
- 15 ~~5. A virtual currency kiosk operator shall issue a refund to a new customer for the full~~
- 16 ~~amount of all transactions made within the thirty day new customer time period on the~~
- 17 ~~request of the customer. To receive a refund under this section, a new customer must~~
- 18 ~~have been fraudulently induced to engage in the virtual currency transactions and~~
- 19 ~~shall contact the virtual currency kiosk operator and a government or law enforcement~~
- 20 ~~regarding the fraudulent nature of the transaction agency within ninety days of the last~~
- 21 ~~transaction to occur during the thirty day new customer time period.~~
- 22 ~~6. A virtual currency kiosk operator shall issue a refund to an existing customer for the~~
- 23 ~~full amount of all transaction fees upon the request of an existing customer. To receive~~
- 24 ~~a refund under this section, a customer must have been fraudulently induced to~~
- 25 ~~engage in the virtual currency transactions and shall contact the virtual currency kiosk~~
- 26 ~~operator and a government or law enforcement agency regarding the fraudulent~~
- 27 ~~nature of the transaction within ninety days of the transaction.~~
- 28 ~~**Daily transaction limit.**~~
- 29 ~~A virtual currency kiosk operator may not accept transactions of more than one thousand~~
- 30 ~~dollars of cash or the equivalent in virtual currency in a day in connection with virtual currency~~



J/13 808 16

~~kiosk transactions with a single customer in this state via one or more virtual currency kiosks  
operated by the same virtual currency operator.~~

~~— **Fee cap.**~~

~~— The aggregate fees and charges, directly or indirectly, charged to a customer related to a  
single transaction or series of related transactions involving virtual currency charged through a  
money transmission kiosk in this state, including any difference between the price charged to a  
customer to buy, sell, exchange, swap, or convert virtual currency and the prevailing market  
value of the virtual currency at the time of the transaction, may not exceed the greater of five  
dollars or three percent of the dollar equivalent of virtual currency involved in the transaction or  
transactions.~~

~~— **Customer service.**~~

~~— A virtual currency kiosk operator performing business in this state shall provide live  
customer service at a minimum on Monday through Friday between eight a.m. central time and  
ten p.m. central time. The customer service toll free number must be displayed on the virtual  
currency kiosk or the virtual currency kiosk screens.~~

**SECTION 1. AMENDMENT.** Section 13-09.1-44 of the North Dakota Century Code is  
amended and reenacted as follows:

**13-09.1-44. Definitions.**

For the purposes of sections 13-09.1-44 through ~~13-09.1-49~~ 13-09.1-54, the following  
definitions apply:

1. "Blockchain analytics" means the analysis of data from blockchains or publicly  
distributed ledgers, including associated transaction information.

2. "Blockchain analytics software" means a software service that uses blockchain  
analytics data to provide risk-specific information about virtual-currency wallet  
addresses.

3. "Control of virtual currency", when used in reference to a transaction or relationship  
involving virtual currency, means the power to execute unilaterally or prevent  
indefinitely a virtual-currency transaction.

2.4. "Exchange", used as a verb, means to assume control of virtual currency from or on  
behalf of a person, at least momentarily, to sell, trade, or convert:



8/3 9 of 16

- 1 a. Virtual currency for money, bank credit, or one or more forms of virtual currency;
- 2 or
- 3 b. Money or bank credit for one or more forms of virtual currency.
- 4 5. "Transaction hash" means a unique identifier made up of a string of characters that act
- 5 as a record and provide proof the transaction was verified and added to the
- 6 blockchain.
- 7 3.6. "Transfer" means to assume control of virtual currency from or on behalf of a person
- 8 and to:
- 9 a. Credit the virtual currency to the account of another person;
- 10 b. Move the virtual currency from one account of a person to another account of the
- 11 same person; or
- 12 c. Relinquish control of virtual currency to another person.
- 13 4.7. "United States dollar equivalent of virtual currency" means the equivalent value of a
- 14 particular virtual currency in United States dollars shown on a virtual-currency
- 15 exchange based in the United States for a particular date or period specified in this
- 16 chapter.
- 17 5.8. "Virtual currency":
- 18 a. Means a digital representation of value that:
- 19 (1) Is used as a medium of exchange, unit of account, or store of value; and
- 20 (2) Is not money, whether or not denominated in money; and
- 21 b. Does not include:
- 22 (1) A transaction in which a merchant grants, as part of an affinity or rewards
- 23 program, value that cannot be taken from or exchanged with the merchant
- 24 for money, bank credit, or virtual currency; or
- 25 (2) A digital representation of value issued by or on behalf of a publisher and
- 26 used solely within an online game, game platform, or family of games sold
- 27 by the same publisher or offered on the same game platform.
- 28 9. "Virtual-currency address" means an alphanumeric identifier associated with a
- 29 virtual-currency wallet identifying the location to which a virtual-currency transaction
- 30 may be sent.



1 ~~6.10.~~ "Virtual-currency administration" means issuing virtual currency with the authority to  
2 redeem the currency for money, bank credit, or other virtual currency.

3 ~~7.11.~~ "Virtual-currency business activity" means:

- 4 a. Exchanging, transferring, or storing virtual currency or engaging in virtual-  
5 currency administration, whether directly or through an agreement with a virtual-  
6 currency control-services vendor;
- 7 b. Holding electronic precious metals or electronic certificates representing interests  
8 in precious metals on behalf of another person or issuing shares or electronic  
9 certificates representing interests in precious metals; or
- 10 c. Exchanging one or more digital representations of value used within one or more  
11 online games, game platforms, or family of games for:
- 12 (1) Virtual currency offered by or on behalf of the same publisher from which  
13 the original digital representation of value was received; or
- 14 (2) Money or bank credit outside the online game, game platform, or family of  
15 games offered by or on behalf of the same publisher from which the original  
16 digital representation of value was received.

17 ~~8.12.~~ "Virtual-currency control-services vendor" means a person that has control of virtual  
18 currency solely under an agreement with a person that, on behalf of another person,  
19 assumes control of virtual currency.

20 13. "Virtual-currency kiosk" means an electronic terminal acting as a mechanical agent of  
21 the virtual-currency kiosk operator to enable the virtual-currency kiosk operator to  
22 facilitate the exchange of virtual currency for money, bank credit, or other virtual  
23 currency, including by:

- 24 a. Connecting directly to a separate virtual-currency exchange that performs the  
25 actual virtual-currency transmission; or
- 26 b. Drawing upon the virtual currency in the possession of the electronic terminal's  
27 operator.

28 14. "Virtual-currency kiosk operator" means a person that engages in virtual-currency  
29 business activity via a money transmission kiosk located in this state or a person that  
30 owns, operates, or manages a money transmission kiosk located in this state through  
31 which virtual-currency business activity is offered.



15. "Virtual-currency kiosk transaction" means:

- a. A transaction conducted or performed, in whole or in part, by electronic means via a virtual-currency kiosk.
- b. A transaction made at a virtual-currency kiosk to purchase virtual currency with fiat currency or to sell virtual currency for fiat currency.

16. "Virtual-currency wallet" means a software application or other mechanism providing a means to hold, store, or transfer virtual currency.

**SECTION 2.** Section 13-09.1-50 of the North Dakota Century Code is created and enacted as follows:

**13-09.1-50. Virtual-currency kiosks.**

1. A kiosk operator may not engage in virtual-currency business activity or hold itself out as being able to engage in virtual-currency business activity with or on behalf of another person unless the kiosk operator is licensed in this state as a money transmitter.
2. A virtual-currency kiosk operator shall comply with all requirements of a money transmitter under this chapter.
3. A virtual-currency kiosk operator may not locate, or allow a third party to locate, a virtual-currency kiosk in this state unless the virtual-currency kiosk:
  - a. Is placed in a commercially accessible area;
  - b. Is accessible to users with sufficient space to account for mobility limitations of users; and
  - c. Is subject to security features, including sufficient lighting and surveillance.
4. Each virtual-currency kiosk operator shall submit a quarterly report of the location of each virtual-currency kiosk located within the state to the commissioner within forty-five days of the end of the calendar quarter. The location report must include:
  - a. The company's legal name;
  - b. Any fictitious or trade name;
  - c. The physical address;
  - d. The start date of operation of the virtual-currency kiosk at the location;
  - e. The end date of operation of the virtual-currency kiosk at the location, if applicable; and



AG 12 of 16

f. The virtual-currency addresses associated with the virtual-currency kiosk.

**SECTION 3.** Section 13-09.1-51 of the North Dakota Century Code is created and enacted as follows:

**13-09.1-51. Disclosures.**

1. A virtual-currency kiosk operator shall disclose in a clear, conspicuous, and easily readable manner in the chosen language of the customer, all relevant terms and conditions generally associated with the products, services, and activities of the virtual-currency kiosk operator and virtual currency.

2. The virtual-currency kiosk operator must receive acknowledgment of receipt of all disclosures required under this section via confirmation of consent.

3. Each virtual-currency kiosk must include a warning written prominently and in bold type, stated in substantially the following form:

a. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:

(1) Claims of a frozen bank account or credit card.

(2) Fraudulent bank transactions.

(3) Claims of identity theft or job offerings in exchange for payments.

(4) Requests for payments to government agencies or companies.

(5) Requests for disaster relief donations or loans.

(6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for vehicles.

(7) Prompts to click on desktop popups, such as virus warnings or communication from alleged familiar merchants.

(8) Communication from someone impersonating a representative of your bank or a law enforcement officer.

(9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW ENFORCEMENT OFFICER BEFORE ANY TRANSACTION.

b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS VIRTUAL-CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE



RISKS AND WISH TO CONTINUE WITH CONDUCTING MY  
VIRTUAL-CURRENCY KIOSK TRANSACTION. PROTECT YOURSELF FROM  
FRAUD. NEVER SEND MONEY TO SOMEONE YOU DO NOT KNOW.

4. The commissioner shall require the disclosure of material risks associated with virtual currency and virtual-currency transactions, including:
  - a. The transaction may not be reversed;
  - b. The virtual-currency kiosk operator's liability for unauthorized virtual currency transactions;
  - c. The virtual-currency kiosk customer's liability for unauthorized currency transactions;
  - d. Virtual currency is not legal tender, backed or insured by the government, and accounts and value balances are not subject to federal deposit insurance corporation, national credit union administration, or securities investor protection corporation protections;
  - e. Some virtual currency transactions are deemed to be made when recorded on a public ledger which may not be the date or time when the individual initiates the transaction;
  - f. Virtual currency's value may be derived from market participants' continued willingness to exchange fiat currency for virtual currency, which may result in the permanent and total loss of a particular virtual currency's value if the market for virtual currency disappears;
  - g. An individual who accepts a virtual currency as payment today is not required to accept and might not accept virtual currency in the future;
  - h. The volatility and unpredictability of the price of virtual currency relative to fiat currency may result in a significant loss over a short period;
  - i. The nature of virtual currency means any technological difficulties experienced by virtual-currency kiosk operators may prevent access to or use of an individual's virtual currency; and
  - j. Any bond maintained by the virtual-currency kiosk operator for the benefit of an individual may not cover all losses an individual incurs.
5. The commissioner shall require disclosure of:



AB 140816

- 1       a.   The amount of the transaction denominated in United States dollars as well as
- 2       the applicable virtual currency.
- 3       b.   Any fees or expenses charged by the virtual-currency kiosk operator.
- 4       c.   Any applicable exchange rates.
- 5       d.   A daily virtual-currency transaction limit of no more than two thousand dollars for
- 6       the first five transactions within the first thirty-day period.
- 7       e.   Notice of a change in the virtual-currency kiosk operator's rules or policies.
- 8       f.   The name, address, and telephone number of the owner of the kiosk and the
- 9       days, time, and means by which a consumer may contact the owner for
- 10      consumer assistance. Any relevant state and local law enforcement agency for
- 11      reporting fraud must be displayed on or at the location of the virtual-currency
- 12      kiosk or on the first screen of the kiosk.
- 13      g.   Under what circumstances the virtual-currency kiosk operator, without a court or
- 14      government order, discloses a person's account information to third parties.
- 15      h.   Other disclosures customarily given in connection with a virtual currency
- 16      transaction.
- 17      6.   After the completion of each transaction, the virtual-currency kiosk operator shall
- 18      provide an individual with a choice of a physical or digital receipt secured with
- 19      two-factor identification in the language chosen by the customer containing the
- 20      following:
- 21      a.   The virtual-currency kiosk operator's name and contact information, including a
- 22      telephone number to answer questions and register complaints;
- 23      b.   The relevant state and local law enforcement or government agency for reporting
- 24      fraud;
- 25      c.   The type, value, date, and precise time of the transaction, transaction hash, and
- 26      each applicable virtual-currency address;
- 27      d.   A unique transaction number able to be linked to the sender during a fraud
- 28      investigation;
- 29      e.   A unique transaction number able to be linked to the designated recipient during
- 30      a fraud investigation;
- 31      f.   All fees charged;



Ag 1504.16

g. The exchange rate of the virtual currency to United States dollars;

h. A statement of the virtual-currency kiosk operator's liability for nondelivery or delayed delivery; and

i. A statement of the virtual-currency kiosk operator's refund policy.

**SECTION 4.** Section 13-09.1-52 of the North Dakota Century Code is created and enacted as follows:

**13-09.1-52. Prevention of fraudulent activity.**

1. A virtual-currency kiosk operator shall use blockchain analytics software to assist in the detection and prevention of suspicious activity, including sending purchased virtual currency from a virtual-currency kiosk operator to a virtual-currency wallet known to be affiliated with fraudulent activity at the time of a transaction and identifying patterns that reflect money laundering or other illicit activity. The commissioner may request evidence from any virtual-currency kiosk operator of use of blockchain analytics.

2. A virtual-currency kiosk operator shall take reasonable steps to detect and prevent fraud, including establishing and maintaining a written antifraud policy. The antifraud policy must include:

a. The identification and assessment of fraud-related risk areas;

b. Procedures and controls to protect against identified risks;

c. Allocation of responsibility for monitoring risks; and

d. Procedures for the periodic evaluation and revision of the antifraud procedures, controls, and monitoring mechanisms.

3. Each virtual-currency kiosk operator shall designate and employ a compliance officer with the following requirements:

a. The individual must be qualified to coordinate and monitor compliance with this chapter and all other applicable federal and state laws and rules;

b. The individual must be employed full-time by the virtual-currency kiosk operator; and

c. The designated compliance officer may not be an individual who owns more than twenty percent of the virtual-currency kiosk operator by whom the individual is employed.



Apr 16 08 16

1 4. Compliance responsibilities required under federal and state laws and rules must be  
2 completed by full-time employees of the virtual-currency kiosk operator.

3 5. A virtual-currency kiosk operator shall maintain, implement, and enforce a written  
4 enhanced due diligence policy. The policy must be reviewed and approved by the  
5 virtual-currency kiosk operator's board of directors or equivalent governing body.

6 6. A virtual-currency kiosk operator shall designate and employ a consumer protection  
7 officer. The consumer protection officer:

8 a. Must be qualified to coordinate and monitor compliance with state and federal  
9 law;

10 b. Must be employed full-time by the virtual-currency kiosk operator; and

11 c. May not own more than twenty percent of the virtual-currency kiosk operator.

12 **SECTION 5.** Section 13-09.1-53 of the North Dakota Century Code is created and enacted  
13 as follows:

14 **13-09.1-53. Daily transaction limit.**

15 A virtual-currency kiosk operator may not accept transactions of more than two thousand  
16 dollars of cash or the equivalent in virtual currency per calendar day for the first five  
17 virtual-currency kiosk transactions occurring within the first thirty-days of the first transaction  
18 with a single customer in this state via one or more virtual-currency kiosks operated by the  
19 same virtual-currency operator.

20 **SECTION 6.** Section 13-09.1-54 of the North Dakota Century Code is created and enacted  
21 as follows:

22 **13-09.1-54. Customer service.**

23 A virtual-currency kiosk operator performing business in this state shall provide live  
24 customer service at a minimum on Monday through Friday between eight a.m. central time and  
25 ten p.m. central time. The customer service toll-free number must be displayed on the  
26 virtual-currency kiosk or the virtual-currency kiosk screens.

**REPORT OF STANDING COMMITTEE  
HB 1447**

**Industry, Business and Labor Committee (Rep. Warrey, Chairman)** recommends **AMENDMENTS** ([25.1011.01002](#)) and when so amended, recommends **DO PASS** (12 YEAS, 0 NAYS, 2 ABSENT AND NOT VOTING). HB 1447 was placed on the Sixth order on the calendar.

25.1011.01002  
Title.

Prepared by the Legislative Council  
staff for Representative Koppelman  
February 12, 2025

Sixty-ninth  
Legislative Assembly  
of North Dakota

## PROPOSED AMENDMENTS TO

### HOUSE BILL NO. 1447

Introduced by

Representatives Swiontek, Christy, Hanson, Heinert, Schauer, J. Olson, Richter

Senators Hogan, Klein, Lee, Rummel, Sickler

1 A BILL ~~for an Act to create and enact a new chapter to title 6 of the North Dakota Century Code,~~  
2 ~~relating to virtual-currency kiosks.~~ for an Act to create and enact sections 13-09.1-50,  
3 13-09.1-51, 13-09.1-52, 13-09.1-53, and 13-09.1-54 of the North Dakota Century Code, relating  
4 to virtual-currency kiosks; and to amend and reenact section 13-09.1-44 of the North Dakota  
5 Century Code, relating to virtual-currency kiosks.

### 6 BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

7 ~~—SECTION 1. A new chapter to title 6 of the North Dakota Century Code is created and~~  
8 ~~enacted as follows:~~

#### 9 ~~—Definitions.~~

10 ~~—In this chapter unless context requires:~~

11 ~~—1. "Blockchain analytics" means the analysis of data from blockchains or public~~  
12 ~~distributed ledgers, including associated transaction information.~~

13 ~~—2. "Blockchain analytics software" means a software service that uses blockchain~~  
14 ~~analytics data to provide risk-specific information about virtual currency wallet~~  
15 ~~addresses.~~

16 ~~—3. "Commissioner" means the commissioner of financial institutions.~~

17 ~~—4. "New customer" means an individual who has never previously transacted with the~~  
18 ~~virtual currency kiosk operator and for the first thirty days after the first financial~~  
19 ~~transaction with the virtual currency kiosk operator.~~

1 — ~~5. "Transaction hash" means a unique identifier made up of a string of characters that act~~  
2 ~~as a record and provide proof the transaction was verified and added to the~~  
3 ~~blockchain.~~

4 — ~~6. "Virtual currency address" means an alphanumeric identifier associated with a virtual~~  
5 ~~currency wallet identifying the location to which a virtual currency transaction can be~~  
6 ~~sent.~~

7 — ~~7. "Virtual currency kiosk" means an electronic terminal acting as a mechanical agent of~~  
8 ~~the virtual currency kiosk operator to enable the virtual currency kiosk operator to~~  
9 ~~facilitate the exchange of virtual currency for money, bank credit, or other virtual~~  
10 ~~currency, including by:~~

11 — ~~a. Connecting directly to a separate virtual currency exchange that performs the~~  
12 ~~actual virtual currency transmission; or~~

13 — ~~b. Drawing upon the virtual currency in the possession of the electronic terminal's~~  
14 ~~operator.~~

15 — ~~8. "Virtual currency kiosk operator" means a person that engages in virtual currency~~  
16 ~~business activity via a money transmission kiosk located in this state or a person that~~  
17 ~~owns, operates, or manages a money transmission kiosk located in this state through~~  
18 ~~which virtual currency business activity is offered.~~

19 — ~~9. "Virtual currency kiosk transaction" means a transaction conducted or performed, in~~  
20 ~~whole or in part, by electronic means via a virtual currency kiosk. Virtual currency~~  
21 ~~kiosk transaction also means a transaction made at a virtual currency kiosk to~~  
22 ~~purchase virtual currency with fiat currency or to sell virtual currency for fiat currency.~~

23 — ~~10. "Virtual currency wallet" means a software application or other mechanism providing a~~  
24 ~~means to hold, store, or transfer virtual currency.~~

25 — **Virtual currency kiosks.**

26 — ~~1. A kiosk operator may not engage in virtual currency business activity or hold itself out~~  
27 ~~as being able to engage in virtual currency business activity with or on behalf of~~  
28 ~~another person unless the kiosk operator is licensed in this state as a money~~  
29 ~~transmitter.~~

30 — ~~2. A virtual currency kiosk operator shall comply with all requirements of a money~~  
31 ~~transmitter under chapter 13-09.1.~~



~~3. A virtual currency kiosk operator may not locate, or allow a third party to locate, a virtual currency kiosk in this state unless the virtual currency kiosk:~~

~~a. Is placed a commercially accessible area;~~

~~b. Is accessible to users with sufficient space to account for mobility limitations of users;~~

~~c. Is subject to security features, including sufficient lighting and surveillance; and~~

~~d. Complies with any additional restrictions or requirements as required by the commissioner.~~

~~4. Each virtual currency kiosk operator shall submit a quarterly report of the location of each virtual currency kiosk located within the state to the commissioner within forty-five days of the end of the calendar quarter. The location report must include:~~

~~a. The company legal name;~~

~~b. Any fictitious or trade name;~~

~~c. The physical address;~~

~~d. The start date of operation of the virtual currency kiosk at the location;~~

~~e. The end date of operation of the virtual currency kiosk at the location, if applicable; and~~

~~f. The virtual currency addresses associated with the virtual currency kiosk.~~

~~**Disclosures.**~~

~~1. A virtual currency kiosk operator shall disclose in a clear, conspicuous, and easily readable manner in the chosen language of the customer, all relevant terms and conditions generally associated with the products, services, and activities of the virtual currency kiosk operator and virtual currency.~~

~~2. The virtual currency kiosk operator must receive acknowledgment of receipt of all disclosures required under this section via confirmation of consent.~~

~~3. Each virtual currency kiosk must include a warning written prominently and in bold type, stating substantially the following form:~~

~~a. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:~~

~~(1) Claims of a frozen bank account or credit card.~~

- 1 ~~\_\_\_\_\_ (2) Fraudulent bank transactions.~~
- 2 ~~\_\_\_\_\_ (3) Claims of identity theft or job offerings in exchange for payments.~~
- 3 ~~\_\_\_\_\_ (4) Requests for payments to government agencies or companies.~~
- 4 ~~\_\_\_\_\_ (5) Requests for disaster relief donations or loans.~~
- 5 ~~\_\_\_\_\_ (6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for~~
- 6 ~~\_\_\_\_\_ vehicles.~~
- 7 ~~\_\_\_\_\_ (7) Prompts to click on desktop popups, such as virus warnings or~~
- 8 ~~\_\_\_\_\_ communication from alleged familiar merchants.~~
- 9 ~~\_\_\_\_\_ (8) Communication from someone impersonating a representative of your bank~~
- 10 ~~\_\_\_\_\_ or a law enforcement officer.~~
- 11 ~~\_\_\_\_\_ (9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL YOUR LOCAL LAW~~
- 12 ~~\_\_\_\_\_ ENFORCEMENT BEFORE ANY TRANSACTION.~~
- 13 ~~\_\_\_\_\_ b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE~~
- 14 ~~\_\_\_\_\_ RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS VIRTUAL~~
- 15 ~~\_\_\_\_\_ CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE RISKS AND~~
- 16 ~~\_\_\_\_\_ WISH TO CONTINUE WITH CONDUCTING MY VIRTUAL CURRENCY KIOSK~~
- 17 ~~\_\_\_\_\_ TRANSACTION. PROTECT YOURSELF FROM FRAUD. NEVER SEND MONEY~~
- 18 ~~\_\_\_\_\_ TO SOMEONE YOU DON'T KNOW.~~
- 19 ~~\_\_\_\_\_ 4. The commissioner shall require the disclosure of material risks associated with virtual~~
- 20 ~~\_\_\_\_\_ currency and virtual currency transactions, including:~~
- 21 ~~\_\_\_\_\_ a. The transaction may not be reversed;~~
- 22 ~~\_\_\_\_\_ b. The virtual currency kiosk operator's liability for unauthorized virtual currency~~
- 23 ~~\_\_\_\_\_ transactions;~~
- 24 ~~\_\_\_\_\_ c. The virtual currency kiosk customer's liability for unauthorized currency~~
- 25 ~~\_\_\_\_\_ transactions;~~
- 26 ~~\_\_\_\_\_ d. Virtual currency is not legal tender, backed or insured by the government, and~~
- 27 ~~\_\_\_\_\_ accounts and value balances are not subject to federal deposit insurance~~
- 28 ~~\_\_\_\_\_ corporation, national credit union administration, or securities investor protection~~
- 29 ~~\_\_\_\_\_ corporation protections;~~

- 1 ~~e. Some virtual currency transactions are deemed to be made when recorded on a~~  
2 ~~public ledger which may not be the date or time when the individual initiates the~~  
3 ~~transaction;~~
- 4 ~~f. Virtual currency's value may be derived from market participants' continued~~  
5 ~~willingness to exchange fiat currency for virtual currency, which may result in the~~  
6 ~~permanent and total loss of a particular virtual currency's value if the market for~~  
7 ~~virtual currency disappears;~~
- 8 ~~g. An individual who accepts a virtual currency as payment today is not required to~~  
9 ~~accept and might not accept virtual currency in the future;~~
- 10 ~~h. The volatility and unpredictability of the price of virtual currency relative to fiat~~  
11 ~~currency may result in a significant loss over a short period;~~
- 12 ~~i. The nature of virtual currency means any technological difficulties experienced by~~  
13 ~~virtual currency kiosk operators may prevent access to or use of an individual's~~  
14 ~~virtual currency; and~~
- 15 ~~j. Any bond maintained by the virtual currency kiosk operator for the benefit of an~~  
16 ~~individual may not cover all losses an individual incurs.~~
- 17 ~~5. The commissioner shall require disclosure of:~~
- 18 ~~a. The amount of the transaction denominated in United States dollars as well as~~  
19 ~~the applicable virtual currency;~~
- 20 ~~b. Any fees or expenses charged by the virtual currency kiosk operator;~~
- 21 ~~c. Any applicable exchange rates;~~
- 22 ~~d. A daily virtual currency transaction limit of no more than one thousand dollars;~~
- 23 ~~e. Notice of a change in the virtual currency kiosk operator's rules or policies;~~
- 24 ~~f. The name, address, and telephone number of the owner of the kiosk and the~~  
25 ~~days, time, means by which a consumer can contact the owner for consumer~~  
26 ~~assistance. Any relevant state and local law enforcement agency for reporting~~  
27 ~~fraud must be displayed on or at the location of the virtual currency kiosk or on~~  
28 ~~the first screen of the kiosk;~~
- 29 ~~g. Under what circumstances the virtual currency kiosk operator, without a court or~~  
30 ~~government order, discloses a person's account information to third parties; and~~

~~h. Other disclosures customarily given in connection with a virtual currency transaction;~~

~~6. After the completion of each transaction, the virtual currency kiosk operator shall provide an individual with a physical receipt in the language chosen by the customer containing the following:~~

~~a. The virtual currency kiosk operator's name and contact information, including a telephone number to answer questions and register complaints;~~

~~b. Relevant state and local law enforcement or government agency for reporting fraud;~~

~~c. The type, value, date, and precise time of the transaction, transaction hash, and each applicable virtual currency address;~~

~~d. The name and contact information of the sender;~~

~~e. The name and contact information of the designated recipient;~~

~~f. All fees charged;~~

~~g. The exchange rate of the virtual currency to United States dollars;~~

~~h. A statement of the virtual currency kiosk operator's liability for nondelivery or delayed delivery;~~

~~i. A statement of the virtual currency kiosk operator's refund policy; and~~

~~j. Any additional information the commissioner may require.~~

~~**Prevention of fraudulent activity.**~~

~~1. A virtual currency kiosk operator shall use blockchain analytics software to assist in the detection and prevention of suspicious activity, including sending purchased virtual currency from a virtual currency kiosk operator to a virtual currency wallet known to be affiliated with fraudulent activity at the time of a transaction and identifying patterns that reflect money laundering or other illicit activity. The commissioner may request evidence from any virtual currency kiosk operator of use of blockchain analytics.~~

~~2. A virtual currency kiosk operator shall take reasonable steps to detect and prevent fraud, including establishing and maintaining a written antifraud policy. The antifraud policy must include:~~

~~a. The identification and assessment of fraud-related risk areas;~~

~~b. Procedures and controls to protect against identified risks;~~

- ~~1 c. Allocation of responsibility for monitoring risks; and~~
- ~~2 d. Procedures for the periodic evaluation and revision of the antifraud procedures,~~
- ~~3 controls, and monitoring mechanisms.~~
- ~~4 3. Each virtual currency kiosk operator shall designate and employ a compliance officer~~
- ~~5 with the following requirements:~~
- ~~6 a. The individual must be qualified to coordinate and monitor compliance with this~~
- ~~7 chapter and all other applicable federal and state laws and rules;~~
- ~~8 b. The individual must be employed full-time by the virtual currency kiosk operator;~~
- ~~9 and~~
- ~~10 c. The designated compliance officer may not be any individual who owns more~~
- ~~11 than twenty percent of the virtual currency kiosk operator by whom the individual~~
- ~~12 is employed.~~
- ~~13 4. Compliance responsibilities required under federal and state laws and rules must be~~
- ~~14 completed by full-time employees of the virtual currency kiosk operator.~~
- ~~15 5. A virtual currency kiosk operator shall issue a refund to a new customer for the full~~
- ~~16 amount of all transactions made within the thirty-day new customer time period on the~~
- ~~17 request of the customer. To receive a refund under this section, a new customer must~~
- ~~18 have been fraudulently induced to engage in the virtual currency transactions and~~
- ~~19 shall contact the virtual currency kiosk operator and a government or law enforcement~~
- ~~20 regarding the fraudulent nature of the transaction agency within ninety days of the last~~
- ~~21 transaction to occur during the thirty-day new customer time period.~~
- ~~22 6. A virtual currency kiosk operator shall issue a refund to an existing customer for the~~
- ~~23 full amount of all transaction fees upon the request of an existing customer. To receive~~
- ~~24 a refund under this section, a customer must have been fraudulently induced to~~
- ~~25 engage in the virtual currency transactions and shall contact the virtual currency kiosk~~
- ~~26 operator and a government or law enforcement agency regarding the fraudulent~~
- ~~27 nature of the transaction within ninety days of the transaction.~~
- ~~28 **Daily transaction limit.**~~
- ~~29 A virtual currency kiosk operator may not accept transactions of more than one thousand~~
- ~~30 dollars of cash or the equivalent in virtual currency in a day in connection with virtual currency~~

~~kiosk transactions with a single customer in this state via one or more virtual currency kiosks  
operated by the same virtual currency operator.~~

~~— **Fee cap.**~~

~~— The aggregate fees and charges, directly or indirectly, charged to a customer related to a  
single transaction or series of related transactions involving virtual currency charged through a  
money transmission kiosk in this state, including any difference between the price charged to a  
customer to buy, sell, exchange, swap, or convert virtual currency and the prevailing market  
value of the virtual currency at the time of the transaction, may not exceed the greater of five  
dollars or three percent of the dollar equivalent of virtual currency involved in the transaction or  
transactions.~~

~~— **Customer service.**~~

~~— A virtual currency kiosk operator performing business in this state shall provide live-  
customer service at a minimum on Monday through Friday between eight a.m. central time and  
ten p.m. central time. The customer service toll free number must be displayed on the virtual  
currency kiosk or the virtual currency kiosk screens.~~

**SECTION 1. AMENDMENT.** Section 13-09.1-44 of the North Dakota Century Code is  
amended and reenacted as follows:

**13-09.1-44. Definitions.**

For the purposes of sections 13-09.1-44 through ~~13-09.1-49~~ 13-09.1-54, the following  
definitions apply:

1. "Blockchain analytics" means the analysis of data from blockchains or publicly  
distributed ledgers, including associated transaction information.

2. "Blockchain analytics software" means a software service that uses blockchain  
analytics data to provide risk-specific information about virtual-currency wallet  
addresses.

3. "Control of virtual currency", when used in reference to a transaction or relationship  
involving virtual currency, means the power to execute unilaterally or prevent  
indefinitely a virtual-currency transaction.

~~2.4.~~ "Exchange", used as a verb, means to assume control of virtual currency from or on  
behalf of a person, at least momentarily, to sell, trade, or convert:

- 1           a. Virtual currency for money, bank credit, or one or more forms of virtual currency;  
2           or  
3           b. Money or bank credit for one or more forms of virtual currency.

4       5. "Transaction hash" means a unique identifier made up of a string of characters that act  
5       as a record and provide proof the transaction was verified and added to the  
6       blockchain.

7       ~~3.6.~~ "Transfer" means to assume control of virtual currency from or on behalf of a person  
8       and to:

- 9           a. Credit the virtual currency to the account of another person;  
10          b. Move the virtual currency from one account of a person to another account of the  
11          same person; or  
12          c. Relinquish control of virtual currency to another person.

13       ~~4.7.~~ "United States dollar equivalent of virtual currency" means the equivalent value of a  
14       particular virtual currency in United States dollars shown on a virtual-currency  
15       exchange based in the United States for a particular date or period specified in this  
16       chapter.

17       ~~5.8.~~ "Virtual currency":

- 18          a. Means a digital representation of value that:  
19             (1) Is used as a medium of exchange, unit of account, or store of value; and  
20             (2) Is not money, whether or not denominated in money; and  
21          b. Does not include:  
22             (1) A transaction in which a merchant grants, as part of an affinity or rewards  
23             program, value that cannot be taken from or exchanged with the merchant  
24             for money, bank credit, or virtual currency; or  
25             (2) A digital representation of value issued by or on behalf of a publisher and  
26             used solely within an online game, game platform, or family of games sold  
27             by the same publisher or offered on the same game platform.

28       9. "Virtual-currency address" means an alphanumeric identifier associated with a  
29       virtual-currency wallet identifying the location to which a virtual-currency transaction  
30       may be sent.



~~6.10.~~ "Virtual-currency administration" means issuing virtual currency with the authority to redeem the currency for money, bank credit, or other virtual currency.

~~7.11.~~ "Virtual-currency business activity" means:

- a. Exchanging, transferring, or storing virtual currency or engaging in virtual-currency administration, whether directly or through an agreement with a virtual-currency control-services vendor;
- b. Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals; or
- c. Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for:
  - (1) Virtual currency offered by or on behalf of the same publisher from which the original digital representation of value was received; or
  - (2) Money or bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received.

~~8.12.~~ "Virtual-currency control-services vendor" means a person that has control of virtual currency solely under an agreement with a person that, on behalf of another person, assumes control of virtual currency.

13. "Virtual-currency kiosk" means an electronic terminal acting as a mechanical agent of the virtual-currency kiosk operator to enable the virtual-currency kiosk operator to facilitate the exchange of virtual currency for money, bank credit, or other virtual currency, including by:

- a. Connecting directly to a separate virtual-currency exchange that performs the actual virtual-currency transmission; or
- b. Drawing upon the virtual currency in the possession of the electronic terminal's operator.

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

15. "Virtual-currency kiosk transaction" means:

- a. A transaction conducted or performed, in whole or in part, by electronic means via a virtual-currency kiosk.
- b. A transaction made at a virtual-currency kiosk to purchase virtual currency with fiat currency or to sell virtual currency for fiat currency.

16. "Virtual-currency wallet" means a software application or other mechanism providing a means to hold, store, or transfer virtual currency.

**SECTION 2.** Section 13-09.1-50 of the North Dakota Century Code is created and enacted as follows:

**13-09.1-50. Virtual-currency kiosks.**

- 1. A kiosk operator may not engage in virtual-currency business activity or hold itself out as being able to engage in virtual-currency business activity with or on behalf of another person unless the kiosk operator is licensed in this state as a money transmitter.
- 2. A virtual-currency kiosk operator shall comply with all requirements of a money transmitter under this chapter.
- 3. A virtual-currency kiosk operator may not locate, or allow a third party to locate, a virtual-currency kiosk in this state unless the virtual-currency kiosk:
  - a. Is placed in a commercially accessible area;
  - b. Is accessible to users with sufficient space to account for mobility limitations of users; and
  - c. Is subject to security features, including sufficient lighting and surveillance.
- 4. Each virtual-currency kiosk operator shall submit a quarterly report of the location of each virtual-currency kiosk located within the state to the commissioner within forty-five days of the end of the calendar quarter. The location report must include:
  - a. The company's legal name;
  - b. Any fictitious or trade name;
  - c. The physical address;
  - d. The start date of operation of the virtual-currency kiosk at the location;
  - e. The end date of operation of the virtual-currency kiosk at the location, if applicable; and

f. The virtual-currency addresses associated with the virtual-currency kiosk.

**SECTION 3.** Section 13-09.1-51 of the North Dakota Century Code is created and enacted as follows:

**13-09.1-51. Disclosures.**

1. A virtual-currency kiosk operator shall disclose in a clear, conspicuous, and easily readable manner in the chosen language of the customer, all relevant terms and conditions generally associated with the products, services, and activities of the virtual-currency kiosk operator and virtual currency.

2. The virtual-currency kiosk operator must receive acknowledgment of receipt of all disclosures required under this section via confirmation of consent.

3. Each virtual-currency kiosk must include a warning written prominently and in bold type, stated in substantially the following form:

a. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A

STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND

THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:

(1) Claims of a frozen bank account or credit card.

(2) Fraudulent bank transactions.

(3) Claims of identity theft or job offerings in exchange for payments.

(4) Requests for payments to government agencies or companies.

(5) Requests for disaster relief donations or loans.

(6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for vehicles.

(7) Prompts to click on desktop popups, such as virus warnings or communication from alleged familiar merchants.

(8) Communication from someone impersonating a representative of your bank or a law enforcement officer.

(9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW ENFORCEMENT OFFICER BEFORE ANY TRANSACTION.

b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE

RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS

VIRTUAL-CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE

RISKS AND WISH TO CONTINUE WITH CONDUCTING MY  
VIRTUAL-CURRENCY KIOSK TRANSACTION. PROTECT YOURSELF FROM  
FRAUD. NEVER SEND MONEY TO SOMEONE YOU DO NOT KNOW.

4. The commissioner shall require the disclosure of material risks associated with virtual  
currency and virtual-currency transactions, including:

a. The transaction may not be reversed;

b. The virtual-currency kiosk operator's liability for unauthorized virtual currency  
transactions;

c. The virtual-currency kiosk customer's liability for unauthorized currency  
transactions;

d. Virtual currency is not legal tender, backed or insured by the government, and  
accounts and value balances are not subject to federal deposit insurance  
corporation, national credit union administration, or securities investor protection  
corporation protections;

e. Some virtual currency transactions are deemed to be made when recorded on a  
public ledger which may not be the date or time when the individual initiates the  
transaction;

f. Virtual currency's value may be derived from market participants' continued  
willingness to exchange fiat currency for virtual currency, which may result in the  
permanent and total loss of a particular virtual currency's value if the market for  
virtual currency disappears;

g. An individual who accepts a virtual currency as payment today is not required to  
accept and might not accept virtual currency in the future;

h. The volatility and unpredictability of the price of virtual currency relative to fiat  
currency may result in a significant loss over a short period;

i. The nature of virtual currency means any technological difficulties experienced by  
virtual-currency kiosk operators may prevent access to or use of an individual's  
virtual currency; and

j. Any bond maintained by the virtual-currency kiosk operator for the benefit of an  
individual may not cover all losses an individual incurs.

5. The commissioner shall require disclosure of:

- a. The amount of the transaction denominated in United States dollars as well as the applicable virtual currency.
  - b. Any fees or expenses charged by the virtual-currency kiosk operator.
  - c. Any applicable exchange rates.
  - d. A daily virtual-currency transaction limit of no more than two thousand dollars for the first five transactions within the first thirty-day period.
  - e. Notice of a change in the virtual-currency kiosk operator's rules or policies.
  - f. The name, address, and telephone number of the owner of the kiosk and the days, time, and means by which a consumer may contact the owner for consumer assistance. Any relevant state and local law enforcement agency for reporting fraud must be displayed on or at the location of the virtual-currency kiosk or on the first screen of the kiosk.
  - g. Under what circumstances the virtual-currency kiosk operator, without a court or government order, discloses a person's account information to third parties.
  - h. Other disclosures customarily given in connection with a virtual currency transaction.
6. After the completion of each transaction, the virtual-currency kiosk operator shall provide an individual with a choice of a physical or digital receipt secured with two-factor identification in the language chosen by the customer containing the following:
- a. The virtual-currency kiosk operator's name and contact information, including a telephone number to answer questions and register complaints;
  - b. The relevant state and local law enforcement or government agency for reporting fraud;
  - c. The type, value, date, and precise time of the transaction, transaction hash, and each applicable virtual-currency address;
  - d. A unique transaction number able to be linked to the sender during a fraud investigation;
  - e. A unique transaction number able to be linked to the designated recipient during a fraud investigation;
  - f. All fees charged;

g. The exchange rate of the virtual currency to United States dollars;

h. A statement of the virtual-currency kiosk operator's liability for nondelivery or delayed delivery; and

i. A statement of the virtual-currency kiosk operator's refund policy.

**SECTION 4.** Section 13-09.1-52 of the North Dakota Century Code is created and enacted as follows:

**13-09.1-52. Prevention of fraudulent activity.**

1. A virtual-currency kiosk operator shall use blockchain analytics software to assist in the detection and prevention of suspicious activity, including sending purchased virtual currency from a virtual-currency kiosk operator to a virtual-currency wallet known to be affiliated with fraudulent activity at the time of a transaction and identifying patterns that reflect money laundering or other illicit activity. The commissioner may request evidence from any virtual-currency kiosk operator of use of blockchain analytics.

2. A virtual-currency kiosk operator shall take reasonable steps to detect and prevent fraud, including establishing and maintaining a written antifraud policy. The antifraud policy must include:

a. The identification and assessment of fraud-related risk areas;

b. Procedures and controls to protect against identified risks;

c. Allocation of responsibility for monitoring risks; and

d. Procedures for the periodic evaluation and revision of the antifraud procedures, controls, and monitoring mechanisms.

3. Each virtual-currency kiosk operator shall designate and employ a compliance officer with the following requirements:

a. The individual must be qualified to coordinate and monitor compliance with this chapter and all other applicable federal and state laws and rules;

b. The individual must be employed full-time by the virtual-currency kiosk operator; and

c. The designated compliance officer may not be an individual who owns more than twenty percent of the virtual-currency kiosk operator by whom the individual is employed.



1        4. Compliance responsibilities required under federal and state laws and rules must be  
2        completed by full-time employees of the virtual-currency kiosk operator.

3        5. A virtual-currency kiosk operator shall maintain, implement, and enforce a written  
4        enhanced due diligence policy. The policy must be reviewed and approved by the  
5        virtual-currency kiosk operator's board of directors or equivalent governing body.

6        6. A virtual-currency kiosk operator shall designate and employ a consumer protection  
7        officer. The consumer protection officer:

8            a. Must be qualified to coordinate and monitor compliance with state and federal  
9            law;

10          b. Must be employed full-time by the virtual-currency kiosk operator; and

11          c. May not own more than twenty percent of the virtual-currency kiosk operator.

12        **SECTION 5.** Section 13-09.1-53 of the North Dakota Century Code is created and enacted  
13 as follows:

14        **13-09.1-53. Daily transaction limit.**

15        A virtual-currency kiosk operator may not accept transactions of more than two thousand  
16        dollars of cash or the equivalent in virtual currency per calendar day for the first five  
17        virtual-currency kiosk transactions occurring within the first thirty-days of the first transaction  
18        with a single customer in this state via one or more virtual-currency kiosks operated by the  
19        same virtual-currency operator.

20        **SECTION 6.** Section 13-09.1-54 of the North Dakota Century Code is created and enacted  
21 as follows:

22        **13-09.1-54. Customer service.**

23        A virtual-currency kiosk operator performing business in this state shall provide live  
24        customer service at a minimum on Monday through Friday between eight a.m. central time and  
25        ten p.m. central time. The customer service toll-free number must be displayed on the  
26        virtual-currency kiosk or the virtual-currency kiosk screens.

**2025 SENATE INDUSTRY AND BUSINESS**

**HB 1447**

# 2025 SENATE STANDING COMMITTEE MINUTES

## Industry and Business Committee Fort Union Room, State Capitol

HB 1447  
3/10/2025

A bill relating to virtual-currency kiosks.
---

10:00 a.m. Chairman Barta opened the hearing.

Member present: Chairman Barta, Vice-Chair Boehm, Senator Klein, Senator Kessel, Senator Enget

### Discussion Topics:

- Increase in fraud and Crypto ATMs
- Seniors, elderly, and vulnerabilities
- Lack of crypto currency understanding
- Examples of crypto-currency fraud within the state
- Suspected unlawful activity and reporting
- Static, un-expiring daily transaction limits and physical receipt requirements
- Crypto kiosk companies fraud liability and victim refunds
- Kiosk operator fee refunding
- Hook, confidence, and sting scams
- Other states and statutes
- AARP, First Western Bank, and CoinFlip
- Location, accessibility, and number of kiosks in the state

10:05 a.m. Lise Kruse, Commissioner, ND Department of Financial Institutions, testified in favor and submitted testimony #39803.

10:15 a.m. Rick Clayburgh, President and CEO, ND Banker's Association, testified in favor and submitted testimony #39752.

10:16 a.m. Jacob Rued, Certified Anti-Money Laundering and Fraud Professional, American Bankers Association, testified in favor and submitted testimony #40009.

10:35 a.m. Ladd Erickson, Attorney, McLean County States, testified in favor and submitted testimony #40008.

10:53 a.m. Janelle Moos, Associate State Director Advocacy, AARP ND, testified in favor and submitted testimony #39788 and #39789.

10:57 a.m. Scott Meske, Bitcoin Depot, testified in favor.

11:00 a.m. John Alexander, Director of Legislative and Regulatory Affairs for the Dakota Credit Union Association (DakCU), testified in favor.

11:03 a.m. Kevin Lolli, Assistant General Counsel for CoinFlip, testified in favor and submitted testimony #39727.

**Additional written testimony:**

Stephanie Engebretson, Chief of Police, Association of ND, submitted testimony #39722 in favor.

11:06 a.m. Chairman Barta closed the hearing.

*Audrey Oswald, Committee Clerk*

March 10, 2025  
Senate Industry and Business  
HB 1447  
Senator Jeff Barta, Chair

For the record, I am Stephanie Dassinger Engebretson, and I am appearing on behalf of the Chiefs of Police Association of North Dakota. I am also the deputy director and attorney for the North Dakota League of Cities.

The Chiefs of Police support HB 1447. This bill creates protective measures for virtual-currency kiosks. This is relatively new financial technology and provides great opportunities for individuals wanting to invest in virtual currencies but also opens up new ways for North Dakotans to fall victim to fraud. Unfortunately, North Dakota has already had residents defrauded using this technology. The Chiefs of Police believe that HB 1447 provides a good step towards helping protect consumers from fraudulent criminal activity using virtual-currency kiosks.

The Chiefs of Police respectfully request a Do Pass recommendation on HB 1447.



**ORAL TESTIMONY SUBMITTED TO THE NORTH DAKOTA  
SENATE INDUSTRY AND BUSINESS COMMITTEE**

**Kevin Lolli, Assistant General Counsel and Consumer Protection Officer  
March 10, 2025**

Chair Barta, Vice-Chair Boehm, and honorable members of the Senate Industry and Business Committee, thank you for the opportunity to provide testimony today regarding HB 1477.

CoinFlip supports the vast majority of HB 1477 relating to the proposed regulation of virtual currency kiosks. However, CoinFlip does support reexamining the time period for a New User. We appreciate the opportunity to offer additional consumer protection-focused recommendations that we know to be highly effective in preventing fraudulent transactions at virtual currency kiosks and look forward to continuing to work with the State of North Dakota to protect consumers.

**Company Background**

CoinFlip is a Chicago-based, global digital currency platform, focused on providing consumers a simple and secure way to buy and sell virtual currency. Founded in 2015, CoinFlip is one of the world's largest operators of virtual currency kiosks, with more than 5,000 locations across the United States and in nine countries around the world, employing more than 200 people.

CoinFlip's kiosks make buying and selling major cryptocurrencies accessible and secure for consumers who wish to purchase their virtual currency using cash. CoinFlip has operated in the State of North Dakota since 2018 and was originally granted a North Dakota money transmitter license by the North Dakota Department of Financial Institutions on October 10, 2023. Additionally, CoinFlip is a money service business ("MSB") registered with the Financial Crimes Enforcement Network. As an MSB, CoinFlip is subject to the Bank Secrecy Act ("BSA"), the United States PATRIOT Act, and their implementing rules and regulations.

CoinFlip embraces licensing regimes as an effective means to create baseline requirements for operations, as well as effective oversight. CoinFlip holds approximately 28 money transmitter licenses with numerous additional applications currently pending. CoinFlip has moved to obtain these licenses, even in states where there is no current licensing requirement.

**Advancing Consumer Protection**

As a company, one of CoinFlip's key business priorities is consumer protection. We won't succeed unless our customers believe we provide them with a safe and secure platform from which to transact virtual currency. CoinFlip's compliance and consumer protection efforts are currently overseen by its Chief Legal Officer, General Counsel, BSA Officer, and Consumer Protection Officer. To effectively manage the risks associated with its operations, CoinFlip implements both



traditional consumer protection efforts such as clear disclosures and warnings, as well as state-of-the-art technology to detect and fight fraudulent transactions.

When transacting with a CoinFlip kiosk, customers are warned numerous times regarding scam-related activity prior to initiating *every* transaction. The customer must attest that they were not sent to the kiosk by a third-party to make a payment; that they are transacting with a digital wallet they own and control; and that they understand all transactions are final and irreversible. This screen is customizable and is updated regularly with warnings about common scams to alert customers and help fight fraud. We also provide clear disclosures on fees and provide customers with a receipt of their transaction via email or text.

Additionally, CoinFlip has 24/7 live customer service and lists its number both on the physical kiosk as well as its transaction screens. Customers are instructed to call CoinFlip in the event a third-party sent them to transact at the kiosk. CoinFlip customer service representatives receive training at least twice annually on AML/BSA requirements and how to be the first line of defense in compliance efforts. As a result of these efforts, CoinFlip's customer support team halted more than 300 potential scams in a four-month period by speaking with the customer who phoned our support team after reading the customer warnings at our kiosk.

CoinFlip also implements state-of-the-art blockchain analytics and compliance tools to block fraudulent transactions and investigate suspicious activity. CoinFlip has automatically blocked more than 1,000 transactions using blockchain analytics in a year's period. In addition to blocking transactions, CoinFlip permanently blacklists digital wallet addresses to prevent those high-risk digital wallets from ever being used at a CoinFlip kiosk again.

### **HB 1447**

The proposed transaction limits in the bill strike a balance between federal reporting requirements and consumer protection. CoinFlip is required to file a Suspicious Activity Report ("SAR") for any suspected suspicious transactions above \$2,000, collect information for the Travel Rule at \$3,000, and file a Currency Transaction Report ("CTR") for transactions above \$10,000. This information is placed in a repository for law enforcement to quickly and accurately conduct investigations.

HB 1477 also includes common sense consumer protections such as fee disclosures, receipt requirements, live customer service, and compliance program standards. CoinFlip knows from experience that these items help protect consumers and deter fraudulent actors. Companies must implement both traditional consumer protections as well as new technology in order to fight bad actors. These protections create a base line for operations in the State of North Dakota for virtual currency kiosk operators that allows responsible companies to continue to operate.

Although, CoinFlip supports the concept of a New Customer, it suggests a change in definition to be more in line with other states. In Minnesota, a New Customer is defined as such for the first 72 hours as a customer. This same model has been passed in the Maryland Senate. Additionally, Nebraska is set to implement a New Customer period that lasts 14 days. CoinFlip suggests North Dakota implement a model that is more in line with the standard set in these states.

## **Proposed Consumer Protection Policies**

CoinFlip believes smart regulation is good for business. CoinFlip has developed the following best practices that would further enhance consumer protections and support their inclusion in any legislation:

- **Require licensure with the state.** CoinFlip believes a money transmitter license should be required for all virtual currency kiosk operators, allowing for state oversight and periodic audits to determine the adequacy of compliance, finance, and cybersecurity programs.
- **Require robust compliance programs.** Kiosk operators should be required to directly employ a qualified, in-house, Chief Compliance Officer and compliance team, that does not have a large ownership interest in the company. At CoinFlip, we take compliance seriously: our Chief Compliance Officer is a former federal prosecutor, and our general counsel is a former Illinois Assistant Attorney General.
- **Require clear, highly visible warnings and fee disclosures.** We agree with the proposed legislation regarding the requirement of clear disclosures regarding all fees and terms of service. We also believe highly visible fraud warnings should be required to be displayed and acknowledged by the customer prior to the initiation and completion of any transaction.
- **Require blockchain analytics.** The use of blockchain analytics technology should be required to fight fraud by automatically blocking customer transactions to high-risk digital wallets.
- **Require live customer service.** Customer service is the first line of defense for consumer protection. We believe every virtual currency kiosk operator should be required to provide trained, live customer service at minimum during business hours.

CoinFlip shares your goals of consumer protection. Although blockchain technology and virtual currency kiosks are new, the fraud we see reported is all too familiar. Whether it's phone, email, text or an online pop-up, scammers repackage the same old tactics and utilize whatever methods they have at hand – Venmo, PayPal, Zelle, Gift Cards, MoneyGram or virtual currency kiosks – to defraud individuals.

The best defense for consumers is to be well-informed and well-alerted at the point of transaction. The best defense for companies is to have the right tools in place to help identify and fight fraud and help law enforcement catch the bad actors.

## **Conclusion**

In conclusion, we believe that a regulatory framework is necessary to protect consumers and encourage innovation and we look forward to working with the North Dakota Senate on HB 1447 to achieve the right balance to protect North Dakota consumers and ensure continued access for lawful virtual currency transactions.

Thank you for your time and consideration.

Sincerely,

/s/ Kevin P. Lolli

Kevin Lolli  
*Assistant General Counsel*



March 10, 2025

Chairman Barta and Members of the Committee, for the record, I am Rick Clayburgh, President and CEO of the North Dakota Banker's Association. The NDBA supports the enactment of **House Bill 1447**, which proposes to regulate crypto-currency kiosk machines here in North Dakota. NDBA supports the amendments offered by the Department of Financial Institutions.

Crypto-currency kiosks, often referred to as Bitcoin ATMs, have seen rapid growth in recent years. At the same time, Bitcoin ATM scams have led to significant consumer financial losses. According to the Federal Trade Commission (FTC), consumers reported losing over \$110 million to such scams in 2023. In the first half of 2024 alone, reported losses exceed \$65 million. These scams often involve fraudsters impersonating government officials, businesses, or tech support, creating a sense of urgency that prompts victims to withdraw cash and deposit it into Bitcoin ATMs.

Notably, the term "ATM" is misleading, as crypto-currency kiosks are not ATMs. ATMs are federally regulated and carry various protections for users. Many people using crypto-currency kiosks are misled into thinking they are protected when the fact is they are not.

HB 1447 aims to address the misuse of crypto-currency kiosks as tools for committing financial crimes with provisions such as:

1. **Licensing and Registration Requirements**
2. **Disclosures**
3. **Fraud Prevention**
4. **Daily Transaction Limits**
5. **Fee Caps**

The regulation of crypto-currency kiosks is a necessary step to ensure that the rapid growth of digital asset platforms does not further compromise consumer protection, legal compliance, or financial stability. Crypto-currency kiosk operators will be held to a standard designed to empower consumers to make informed decisions, thereby fostering trust and collaboration within the financial ecosystem of our state.

***NDBA Requests the committee adopt the amendments presented by DFI and place a do-pass recommendation on HB 1447.***

Thank you

Google Maps

cryptocurrency atm

Bismarck



Map data ©2025 Google 1 mi

Hours ▾

All filters

## Results ⓘ

## Sponsored

## Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 🚶 · 706 Kirkwood Mall

Opens soon · 11AM ·

(678) 435-9604



Website



Directions

## Locate The Closest Bitcoin ATM

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ ATM locations....

[Visit Site](#)

## Sponsored

## RockItCoin Bitcoin ATM

No reviews

Crypto ATM · 🚶 · 2921 N 11th St



Website



Directions



Open · Closes 11 PM ·

(888) 702-4826

### BTC ATM

Use "EARN10" Promo Code at RockItCoin®

**ATMs** & Earn an Extra \$10 Bitcoin in Your...

[Visit Site](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 1144 E Bismarck Expy

Open · Closes 12 AM · (701) 401-3888



[Directions](#)

### Cryptobase Bitcoin ATM

No reviews

ATM · [📍](#) · 406 N 6th St

Open 24 hours · (301) 702-0115



[Website](#)



[Directions](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 4400 Ottawa St

Open · Closes 12 AM · (701) 401-5286



[Directions](#)

### LibertyX Bitcoin ATM

No reviews

ATM · 406 N 6th St

Open 24 hours · (800) 511-8940



[Website](#)



[Directions](#)

### Bitcoin ATM Bismarck-Cryptobase

No reviews

ATM · [📍](#) · 4100 Saratoga Ave

Open 24 hours · (305) 702-0115



[Website](#)



[Directions](#)

### Coinstar Kiosk - Bitcoin ATM

No reviews

ATM · [📍](#) · 1144 E Bismarck Expy

Coborn's

Open · Closes 5 PM ·



[Website](#)



[Directions](#)

Google Maps

cryptocurrency atms in fargo



Map data ©2025 Google 1 mi

Hours ▾

All filters

Results ⓘ


Showing results for **cryptocurrency** atms in fargo. Search instead for **cyrpotcurrency** atms in fargo.


Sponsored

RockItCoin Bitcoin ATM

3.0 (1)

Crypto ATM · 📍 · 950 13th Ave E  
Open 24 hours · (888) 702-4826

 Website

 Directions

Bitcoin ATM Near Me


Use "EARN10" Promo Code at RockItCoin® [Visit Site](#)  
ATM & Get Extra \$10 of Bitcoin on...


Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 📍 · 1210 13th Ave E

 Website

 Directions

**Open 24 hours** · (678) 435-9604

**15,000+ Locations Nationwide**

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM** locations. 24...

[Visit Site](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 1401 33rd St S

**Open** · Closes 12AM · (218) 789-8292



[Directions](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 📍 · 755 33rd Ave E

**Open** · Closes 12AM · (701) 929-6588



[Directions](#)

### CoinFlip Bitcoin ATM

5.0 (3)

ATM · 📍 · 3021 13th Ave S Unit 1

**Open** · Closes 9 PM ·

(773) 800-0106



[Website](#)



[Directions](#)

### Coin Cloud Bitcoin ATM

No reviews

ATM · 4907 Timber Pkwy S

**Open** · Closes 12AM · (701) 369-9740



[Directions](#)

### Coinsource Bitcoin ATM

No reviews

ATM · 📍 · 3441 13th Ave S

**Open** · Closes 9 PM ·

(805) 500-2646



[Website](#)



[Directions](#)

### Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 📍 · 3040 25th St S

**Open 24 hours** · (678) 435-9604



[Website](#)



[Directions](#)



## cryptocurrency atm near Dickinson nd



Map data ©2025 Google 2000 ft

Hours ▾

🔍 All filters

### Results ⓘ

#### Sponsored

##### Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 797 S Main Ave

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

##### Bitcoin ATM Promo Code

New Customer Promo Special! Buy Bitcoin with Cash at over 15,000+ Bitcoin Depot...

[Visit Site](#)

#### Sponsored

##### Byte Federal Bitcoin ATM (Arco)

5.0 (2)

Crypto ATM · 🚗 · 450 12th St W



Website



Directions



**Bitcoin ATM Locations Near You**

Bitcoin **ATM Near Me** - Search for the  
USA's Best Crypto **ATMs** - Highest Limits...

[Visit Site](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 📍 · 1761 3rd Ave W

**Open** · Closes 11PM · (701) 502-4647

[Directions](#)**Byte Federal Bitcoin ATM  
(Arco)**

5.0 (2)

Crypto ATM · 📍 · 450 12th St W

**Open** · Closes 10 PM ·

(786) 686-2983

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 797 S Main Ave

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 191 40th St W

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 1005 E Villard St

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Coinstar Kiosk - Bitcoin ATM**

3.0 (2)

ATM · 📍 · 1761 3rd Ave W Coborn's

**Open** · Closes 10 PM ·

(800) 928-2274

[Website](#)[Directions](#)





cryptocurrency atm near minot, nd



Map data ©2025 Google 1 mi

Hours ▾

All filters

## Results ⓘ

Showing results for **cryptocurrency** atm near minot, nd. Search instead for **cryptocurrency** atm near minot, nd.

## Sponsored

## Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 🚶 · 1512 4th Ave NW

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

15,000+ Locations Nationwide

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM** locations. 24...

Visit Site

## Sponsored

**RockItCoin Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 2025 3rd St NW

**Open** · Closes 8 PM ·

(888) 702-4826

[Website](#)[Directions](#)**Bitcoin ATM Near Me**

Use "EARN10" Promo Code at RockItCoin®

[Visit Site](#)

ATM &amp; Get Extra \$10 of Bitcoin on...

**Bitcoin Depot - Bitcoin ATM**

5.0 (1)

Crypto ATM · 📍 · 301 40th Ave SW

**Open** · Closes 11 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Coinsource Bitcoin ATM**

5.0 (1)

ATM · 1520 24th Ave SW

**Open 24 hours** · (805) 500-2646[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 1512 4th Ave NW

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 409 E Burdick

Expy

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 810 N Broadway

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 2400 10th St SW

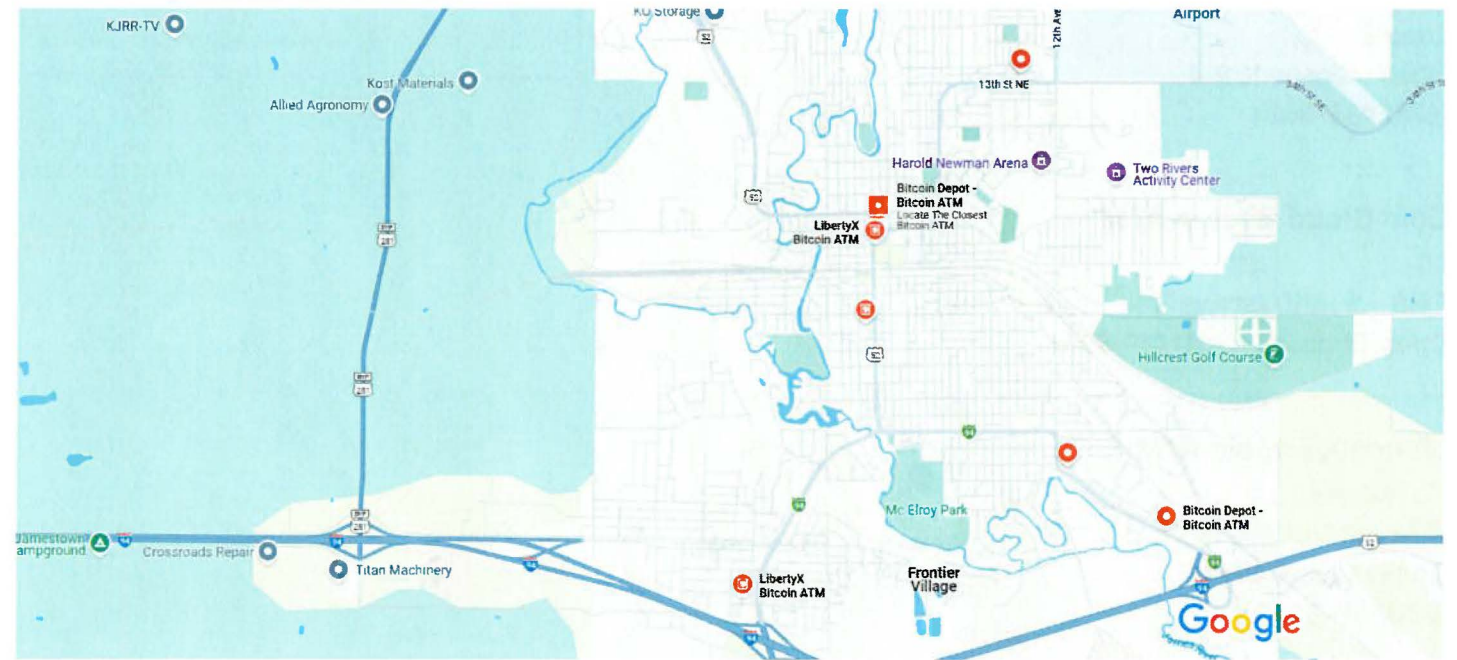
**Open** · Closes 7 PM ·

(678) 435-9604

[Website](#)[Directions](#)



cryptocurrency atm near jamestown, nd



Map data ©2025 Google 2000 ft

Hours ▾

☰ All filters

Results ⓘ

Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 424 1st Ave N

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

Locate The Closest Bitcoin ATM

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ ATM locations. 24...

Visit Site

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 424 1st Ave N

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 📍 · 1609 Business Loop E

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)**Coin Cloud Bitcoin ATM**

1.0 (1)

ATM · 📍 · 310 1st Ave S

**Open 24 hours** · (701) 419-8894[Website](#)[Directions](#)**LibertyX Bitcoin ATM**

No reviews

ATM · 424 1st Ave N

**Open** · Closes 10 PM ·

(800) 511-8940

[Website](#)[Directions](#)**LibertyX Bitcoin ATM**

No reviews

Crypto ATM · 1219 Business Loop E  
(800) 511-8940[Directions](#)**Buy Bitcoin**

No reviews

Crypto ATM · 📍 · 1003 13th St NE  
(888) 212-5824[Website](#)[Directions](#)**Buy Bitcoin**

No reviews

Crypto ATM · 📍 · 1219 Business Loop E

(888) 212-5824

[Website](#)[Directions](#)





cryptocurrency atm near grand forks, nd



Map data ©2025 Google 2000 ft

Hours ▾

🏠 All filters

Results ⓘ

Sponsored

Bitcoin Depot - Bitcoin ATM

No reviews

Crypto ATM · 4250 University Ave

Open · Closes 10 PM ·

(678) 435-9604



Website



Directions

Locate The Closest Bitcoin ATM

Make Hassle-Free Bitcoin Purchases with Bitcoin Depot. 8,000+ **ATM** locations. 24...

Visit Site

Sponsored

CoinFlip Bitcoin ATM

1.0 (1)

ATM · 🏠 · 4220 5th Ave N

Open · Closes 11 PM ·

(773) 800-0106



Website



Directions

**Coin Cloud Bitcoin ATM**

5.0 (1)

ATM · 📍 · 1750 32nd Ave S

**Open** · Closes 10 PM · (701) 987-3073[Directions](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 📍 · 1631 S Washington St

**Open** · Closes 10 PM · (701) 765-5004[Directions](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 📍 · 1315 S Columbia Rd

**Open** · Closes 10 PM · (701) 765-5298[Directions](#)**Coin Cloud Bitcoin ATM**

No reviews

ATM · 📍 · 1925 13th Ave N

**Open** · Closes 10 PM · (701) 402-5582

Onsite services

[Directions](#)**Bitcoin Depot - Bitcoin ATM**

1.0 (1)

Crypto ATM · 📍 · 3450 32nd Ave S

**Open 24 hours** · (678) 435-9604[Website](#)[Directions](#)**Bitcoin Depot - Bitcoin ATM**

No reviews

Crypto ATM · 4326 Gateway Dr

**Open** · Closes 10 PM ·

(678) 435-9604

[Website](#)[Directions](#)



Engrossed House Bill 1447 – Support  
March 10, 2025  
Senate Industry and Business Committee  
Janelle Moos, AARP [jmoos@aarp.org](mailto:jmoos@aarp.org)

Chairman Barta and members of the Senate Industry and Business Committee,

My name is Janelle Moos, Associate State Director of Advocacy, with AARP North Dakota. AARP is a nonpartisan, nonprofit, nationwide organization with nearly 38 million members. Approximately, 82,000 of those members live in North Dakota. I'm here to testify in support of Engrossed HB 1447, including the amendments proposed by the Department of Financial Institutions regarding the daily transaction limit.

Scams involving cryptocurrency ATMs are on the rise—and AARP ND is urging you to take action this legislative session. HB 1447, sponsored by Representative Swiontek, will create important consumer protections to save older North Dakotans from having their hard-earned money, sometimes their life savings, stolen by criminals misusing crypto kiosks or “ATMs” for fraudulent activity.

Cryptocurrency fraud has taken a quantum leap in recent years. The FBI says that in 2023, Americans reported losing more than \$5.6 billion through fraud involving cryptocurrency, North Dakotans lost over \$6 million in cryptocurrency fraud. One area of growth is in payments using cryptocurrency ATMs, also known as “crypto kiosks” or “virtual currency kiosks.” These devices can be found in supermarkets, convenience stores, gas stations, bars, restaurants, and shopping malls. Today, there are more than 45,000 crypto ATMs nationwide. Attached to the testimony are maps of where some of these machines are located in North Dakota.

Because crypto ATMs are still relatively new and largely unregulated at the state level compared to traditional financial institutions and money service businesses, they lack sufficient consumer fraud protections. As a result, criminals are using crypto ATMs to steal hundreds of millions of dollars from Americans each year through fraudulent purchase schemes. In the same report referenced above, the FBI received over 5,500 complaints involving crypto kiosks, and Americans reported over \$189 million in stolen funds. Fraud is significantly underreported, so the amount stolen is likely far higher.

Perpetrators convince individuals that they must address an urgent matter, directing them to withdraw large amounts of cash from their banks. The individual then inserts that money into a

crypto “ATM” and is told to direct the money to a “secure wallet.” Once the payment is made it’s transferred to the criminal and virtually untraceable. We have included a copy of one email we recently received directing a local Bismarck resident to keep some internet searches private by making a payment at a cryptocurrency kiosk. This resident understood the warning signs and shared the email so we could help others.

As Representative Swiontek mentioned in his testimony, HB 1447 is designed to prevent North Dakotans from losing their savings to criminals by implementing important consumer protections including:

- **Licensing cryptocurrency kiosk operators in the state.** This is accomplished in section 2 of the bill specifically starting on page 4 line 7. Currently, North Dakota statute could use some clarity on requiring cryptocurrency kiosk operators to be licensed in North Dakota. This section would make it clear that they require licensure under the ND Department of Financial Institutions as a money transmitter. It also ensures that operators locate the kiosks in commercial areas and submit quarterly reports.
- **Posting fraud warning notices that are visible and identify steps people should take if they suspect fraudulent activity.** Because these crypto kiosks can look like bank ATMs, including disclosures and warnings is an important consumer protection. The language on page 5 lines 8-31, outline the notice that operators would be required to post and prompts to notify law enforcement if they suspect fraud. Additional disclosure requirements are on pages 6-7.
- **Clearly displaying terms and conditions before a transaction, including any fees charged and the exchange rate.** You can find these requirements spelled out on page 6 and continuing onto page 7 lines 1-13 .
- **Giving receipts with relevant transactional information.** Page 7, lines 14-31, make it clear that crypto kiosk operators must provide paper or digital receipts with the operator’s name and contact information, relevant state and local law enforcement in which to report fraud, the transaction details like sender and recipient names, transaction values and data, fee amounts. These and the other items aid law enforcement being able to investigate immediately, helping in victim recovery efforts.
- **Imposing daily transaction limits to avoid potential risks associated with higher transactions.** Page 9, lines 12-17 specifies a \$2,000 limit on daily transactions per vendor. Currently, we are unaware of daily limits on transactions using cryptocurrency kiosks and we’ve been made aware of North Dakotans that have lost as much as \$25,000 in one transaction. We support the amendment proposed by the Department of Financial Institutions that removes the 5 transactions over a 30 day period.

AARP regularly provides free timely information to consumers and their families through the work of our AARP Fraud Watch Network ([aarp.org/fraud](http://aarp.org/fraud)). In North Dakota alone, we regularly



provide consumer updates via media partnerships, free shredding events, educational community events, telephone townhalls, webinars, and volunteer presentations. We also support laws and regulations that strengthen and enhance consumer protections, like those contained in HB 1447.

Fraud and other financial crimes, including cryptocurrency kiosk/ATM fraud, create real financial devastation —billions of dollars are lost each year. The impact of fraud on victims and their families is wide reaching and emotionally devastating, especially for older Americans. It's a crime that deserves more attention and effort to combat. **AARP North Dakota strongly supports protections against fraud, and we urge you to support HB 1447.**

Thank you.



## MEMORANDUM

**DATE:** March 10, 2025

**TO:** Senate Industry and Business Committee

**FROM:** Lise Kruse, Commissioner

**SUBJECT:** Testimony in Support of House Bill No. 1447

Chairman Barta and members of the Senate Industry and Business Committee, thank you for the opportunity to testify in support of House Bill No. 1447.

Our department oversees banks, credit unions, trust companies, and other nonbank financial corporations such as money transmitters and lenders. The department is in support of this Bill since it clarifies an area where we already have jurisdiction. Oversight of virtual currency money transmitters is outlined in NDCC 13-09.1 and this would be an add-on to that model law that legislature approved in 2023. The department had already planned on expanding and clarifying that section, related to crypto ATMs, and therefore we were pleased to work with AARP on this topic.

There has been an increase in fraud in recent years, and banks have alerted me to the increase in financial elder abuse, and now specifically, how grandma is duped into putting cash into a crypto ATM, often with help from the fraudsters, and the money is gone. Crypto ATMs have become the new avenue for fraudsters, instead of gift cards which was the fraudsters' currency of choice, this is faster since the cash loaded into a crypto ATM is instantaneously in the fraudster's crypto wallet. Due to the potential for fraud, I believe it is appropriate to enforce some type of limit, better consumer alerts at the machines, and clarify what the ATM owners are required to do to help prevent fraudulent transactions.

Per the FBI Internet Crime Complaint Center, total crypto fraud losses jumped 45% in 2023 to \$5.6 billion. The center reported over 69,000 complaints, with 17,000 complaints from people over the age of 60, with losses of \$1.6 billion. North Dakota complaints totaled 103 with \$6.5 million in losses, which is over \$60,000 per person on average. In the FBI report, crypto ATMs accounted for more than 5,000 complaints with losses of \$189 million. Over half the complaints were from individuals over the age of 60 and resulted in \$124 million of the losses. These numbers are likely low, since many victims, especially in our elderly population, are hesitant to report it due to embarrassment. A reason why the fraud victims with crypto ATMs

are predominantly elderly is likely due to the fact that younger individuals active in the crypto marketplace uses exchanges on their phone and would not need a physical location.

Testimony submitted in opposition during the house hearing raised a concern that this Bill will somehow lessen a company's obligation to report suspicious activity to government and law enforcement. If you hear things like that today, please know that is not the case. Federal law requires that any suspicious activity for a money service business is reported on transactions if it "involves or aggregates funds or other assets of at least \$2,000." That does not mean that transactions would need to reach \$2,000 before any suspected unlawful activity is reported. The statute also states that "Any money services business may also file...a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by this section" CFR 31 1022.320(a).

We are requesting an amendment to correct a few issues that have raised concern. When it was voted on at the House floor, questions were raised regarding the definitions. We have looked at what other states have and what has been proposed on the federal level and have the following suggestions:



On page 1, the first two definitions were combined in a proposed federal bill, and I suggest using that for simplicity rather than having a separate definition adding “software”. Definition 14 on page 3 introduced a new term “money transmission kiosk”. I shortened it to match what Minnesota has, which is clear and concise.

Also, the House did considerable work on this Bill, which resulted in substantial changes. These changes include raising the transaction limit from \$1,000 to \$2,000, removing the crypto kiosk companies’ fraud liability, eliminating a maximum fee the crypto kiosk companies can charge North Dakota consumers, and modification of the requirement to provide North Dakota customers a paper receipt. One change is especially problematic and makes this statute less effective as a fraud protection, that is the change to the daily limits. On page 7 lines 2-3 and the last page (page 9) lines 14-15, language was inserted to make limitations only for the first 5 transactions within the first 30 days of the first transaction. This would only limit someone if they are a victim of a fraud the first few times they use this machine. Also, it ignores the fact that many victims are victims over time, such as romance scam victims. Also, fraudsters can easily circumvent these limitations by keeping the amounts low in the beginning and increasing amounts over time. For these reasons, we are requesting an amendment here to address this

fraud risk, to ensure this Bill provides effective fraud protection. This change back to a more reasonable transaction limit would be consistent with laws in other states.

Finally, there are people here today that work with fraud victims every day and see the concerning activities that this Bill is trying to address. The people that are victims that we want to protect are North Dakota citizens, losing substantial amounts of money. Therefore, we request a “do pass” on this Bill including a “do pass” on the proposed amendment.

Mr. Chairman, thank you for the opportunity to provide this testimony. I would be happy to answer any questions the Committee may have.

**FIRST ENGROSSMENT**

**ENGROSSED HOUSE BILL NO. 1447**

Introduced by

Representatives Swiontek, Christy, Hanson, Heinert, Schauer, J. Olson, Richter

Senators Hogan, Klein, Lee, Rummel, Sickler

1 A BILL for an Act to create and enact sections 13-09.1-50, 13-09.1-51, 13-09.1-52, 13-09.1-53,  
2 and 13-09.1-54 of the North Dakota Century Code, relating to virtual-currency kiosks; and to  
3 amend and reenact section 13-09.1-44 of the North Dakota Century Code, relating to virtual-  
4 currency kiosks.

5 **BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

6 **SECTION 1. AMENDMENT.** Section 13-09.1-44 of the North Dakota Century Code is  
7 amended and reenacted as follows:

8 **13-09.1-44. Definitions.**

9 For the purposes of sections 13-09.1-44 through ~~13-09.1-49~~13-09.1-54, the following  
10 definitions apply:

- 11 1. "Blockchain analytics" means the analysis of data from blockchains or publicly  
12 distributed ledgers, including associated transaction information—  
13 ~~2. "Blockchain analytics software" means a software service that uses blockchain~~  
14 ~~analytics data~~ to provide risk-specific information about virtual-currency transactions and  
15 virtual currency wallet addresses.  
16 3. "Control of virtual currency", when used in reference to a transaction or relationship  
17 involving virtual currency, means the power to execute unilaterally or prevent  
18 indefinitely a virtual-currency transaction.  
19 ~~2.4.~~ "Exchange", used as a verb, means to assume control of virtual currency from or on  
20 behalf of a person, at least momentarily, to sell, trade, or convert:  
21 a. Virtual currency for money, bank credit, or one or more forms of virtual currency;  
22 or

b. Money or bank credit for one or more forms of virtual currency.

5. "Transaction hash" means a unique identifier made up of a string of characters that act as a record and provide proof the transaction was verified and added to the blockchain.

~~3.6.~~ "Transfer" means to assume control of virtual currency from or on behalf of a person and to:

a. Credit the virtual currency to the account of another person;

b. Move the virtual currency from one account of a person to another account of the same person; or

c. Relinquish control of virtual currency to another person.

4.7. "United States dollar equivalent of virtual currency" means the equivalent value of a particular virtual currency in United States dollars shown on a virtual-currency exchange based in the United States for a particular date or period specified in this chapter.

~~5.8.~~ "Virtual currency":

a. Means a digital representation of value that:

(1) Is used as a medium of exchange, unit of account, or store of value; and

(2) Is not money, whether or not denominated in money; and

b. Does not include:

(1) A transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for money, bank credit, or virtual currency; or

(2) A digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.

9. "Virtual-currency address" means an alphanumeric identifier associated with a virtual-currency wallet identifying the location to which a virtual-currency transaction may be sent.

~~6.10.~~ "Virtual-currency administration" means issuing virtual currency with the authority to redeem the currency for money, bank credit, or other virtual currency.

~~7.11.~~ "Virtual-currency business activity" means:



- a. Exchanging, transferring, or storing virtual currency or engaging in virtual-currency administration, whether directly or through an agreement with a virtual-currency control-services vendor;
- b. Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals; or
- c. Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for:
  - (1) Virtual currency offered by or on behalf of the same publisher from which the original digital representation of value was received; or
  - (2) Money or bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received.

~~8-12.~~ "Virtual-currency control-services vendor" means a person that has control of virtual currency solely under an agreement with a person that, on behalf of another person, assumes control of virtual currency.

13. "Virtual-currency kiosk" means an electronic terminal acting as a mechanical agent of the virtual-currency kiosk operator to enable the virtual-currency kiosk operator to facilitate the exchange of virtual currency for money, bank credit, or other virtual currency, including by:

- a. Connecting directly to a separate virtual-currency exchange that performs the actual virtual-currency transmission; or
- b. Drawing upon the virtual currency in the possession of the electronic terminal's operator.

~~14. "Virtual-currency kiosk operator" means a person that engages in virtual-currency business activity via a money transmission kiosk located in this state or a person that owns, operates, or manages a money transmission kiosk located in this state through which virtual-currency business activity is offered. that operates a virtual currency kiosk within North Dakota.~~

15. "Virtual-currency kiosk transaction" means:

- a. A transaction conducted or performed, in whole or in part, by electronic means via a virtual-currency kiosk.

- 1           b. A transaction made at a virtual-currency kiosk to purchase virtual currency with  
2           fiat currency or to sell virtual currency for fiat currency.

- 3       16. "Virtual-currency wallet" means a software application or other mechanism providing a  
4       means to hold, store, or transfer virtual currency.

5       **SECTION 2.** Section 13-09.1-50 of the North Dakota Century Code is created and enacted  
6 as follows:

7       **13-09.1-50. Virtual-currency kiosks.**

- 8       1. A kiosk operator may not engage in virtual-currency business activity or hold itself out  
9       as being able to engage in virtual-currency business activity with or on behalf of  
10       another person unless the kiosk operator is licensed in this state as a money  
11       transmitter.

- 12       2. A virtual-currency kiosk operator shall comply with all requirements of a money  
13       transmitter under this chapter.

- 14       3. A virtual-currency kiosk operator may not locate, or allow a third party to locate, a  
15       virtual-currency kiosk in this state unless the virtual-currency kiosk:

- 16           a. Is placed in a commercially accessible area;

- 17           b. Is accessible to users with sufficient space to account for mobility limitations of  
18           users; and

- 19           c. Is subject to security features, including sufficient lighting and surveillance.

- 20       4. Each virtual-currency kiosk operator shall submit a quarterly report of the location of  
21       each virtual-currency kiosk located within the state to the commissioner within  
22       forty-five days of the end of the calendar quarter. The location report must include:

- 23           a. The company's legal name;

- 24           b. Any fictitious or trade name;

- 25           c. The physical address;

- 26           d. The start date of operation of the virtual-currency kiosk at the location;

- 27           e. The end date of operation of the virtual-currency kiosk at the location, if  
28           applicable; and

- 29           f. The virtual-currency addresses associated with the virtual-currency kiosk.

30       **SECTION 3.** Section 13-09.1-51 of the North Dakota Century Code is created and enacted  
31 as follows:

**13-09.1-51. Disclosures.**

1. A virtual-currency kiosk operator shall disclose in a clear, conspicuous, and easily readable manner in the chosen language of the customer, all relevant terms and conditions generally associated with the products, services, and activities of the virtual-currency kiosk operator and virtual currency.
2. The virtual-currency kiosk operator must receive acknowledgment of receipt of all disclosures required under this section via confirmation of consent.
3. Each virtual-currency kiosk must include a warning written prominently and in bold type, stated in substantially the following form:

  - a. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:

    - (1) Claims of a frozen bank account or credit card.
    - (2) Fraudulent bank transactions.
    - (3) Claims of identity theft or job offerings in exchange for payments.
    - (4) Requests for payments to government agencies or companies.
    - (5) Requests for disaster relief donations or loans.
    - (6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for vehicles.
    - (7) Prompts to click on desktop popups, such as virus warnings or communication from alleged familiar merchants.
    - (8) Communication from someone impersonating a representative of your bank or a law enforcement officer.
    - (9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW ENFORCEMENT OFFICER BEFORE ANY TRANSACTION.
  - b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS VIRTUAL-CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE RISKS AND WISH TO CONTINUE WITH CONDUCTING MY VIRTUAL-CURRENCY KIOSK TRANSACTION. PROTECT YOURSELF FROM FRAUD. NEVER SEND MONEY TO SOMEONE YOU DO NOT KNOW.

- 1       4.   The commissioner shall require the disclosure of material risks associated with virtual  
2       currency and virtual-currency transactions, including:
- 3       a.   The transaction may not be reversed;  
4       b.   The virtual-currency kiosk operator's liability for unauthorized virtual currency  
5       transactions;  
6       c.   The virtual-currency kiosk customer's liability for unauthorized currency  
7       transactions;  
8       d.   Virtual currency is not legal tender, backed or insured by the government, and  
9       accounts and value balances are not subject to federal deposit insurance  
10      corporation, national credit union administration, or securities investor protection  
11      corporation protections;  
12      e.   Some virtual currency transactions are deemed to be made when recorded on a  
13      public ledger which may not be the date or time when the individual initiates the  
14      transaction;  
15      f.   Virtual currency's value may be derived from market participants' continued  
16      willingness to exchange fiat currency for virtual currency, which may result in the  
17      permanent and total loss of a particular virtual currency's value if the market for  
18      virtual currency disappears;  
19      g.   An individual who accepts a virtual currency as payment today is not required to  
20      accept and might not accept virtual currency in the future;  
21      h.   The volatility and unpredictability of the price of virtual currency relative to fiat  
22      currency may result in a significant loss over a short period;  
23      i.   The nature of virtual currency means any technological difficulties experienced by  
24      virtual-currency kiosk operators may prevent access to or use of an individual's  
25      virtual currency; and  
26      j.   Any bond maintained by the virtual-currency kiosk operator for the benefit of an  
27      individual may not cover all losses an individual incurs.
- 28      5.   The commissioner shall require disclosure of:
- 29      a.   The amount of the transaction denominated in United States dollars as well as  
30      the applicable virtual currency.  
31      b.   Any fees or expenses charged by the virtual-currency kiosk operator.



- 1           c. Any applicable exchange rates.
- 2           d. A daily virtual-currency transaction limit of no more than two thousand dollars ~~for~~  
3           ~~the first five transactions within the first thirty-day period~~ per day.
- 4           e. Notice of a change in the virtual-currency kiosk operator's rules or policies.
- 5           f. The name, address, and telephone number of the owner of the kiosk and the  
6           days, time, and means by which a consumer may contact the owner for  
7           consumer assistance. Any relevant state and local law enforcement agency for  
8           reporting fraud must be displayed on or at the location of the virtual-currency  
9           kiosk or on the first screen of the kiosk.
- 10          g. Under what circumstances the virtual-currency kiosk operator, without a court or  
11          government order, discloses a person's account information to third parties.
- 12          h. Other disclosures customarily given in connection with a virtual currency  
13          transaction.
- 14          6. After the completion of each transaction, the virtual-currency kiosk operator shall  
15          provide an individual with a choice of a physical or digital receipt secured with  
16          two-factor identification in the language chosen by the customer containing the  
17          following:
  - 18           a. The virtual-currency kiosk operator's name and contact information, including a  
19           telephone number to answer questions and register complaints;
  - 20           b. The relevant state and local law enforcement or government agency for reporting  
21           fraud;
  - 22           c. The type, value, date, and precise time of the transaction, transaction hash, and  
23           each applicable virtual-currency address;
  - 24           d. A unique transaction number able to be linked to the sender during a fraud  
25           investigation;
  - 26           e. A unique transaction number able to be linked to the designated recipient during  
27           a fraud investigation;
  - 28           f. All fees charged;
  - 29           g. The exchange rate of the virtual currency to United States dollars;
  - 30           h. A statement of the virtual-currency kiosk operator's liability for nondelivery or  
31           delayed delivery; and

i. A statement of the virtual-currency kiosk operator's refund policy.

**SECTION 4.** Section 13-09.1-52 of the North Dakota Century Code is created and enacted  
as follows:

**13-09.1-52. Prevention of fraudulent activity.**

1. A virtual-currency kiosk operator shall use blockchain analytics software to assist in the detection and prevention of suspicious activity, including sending purchased virtual currency from a virtual-currency kiosk operator to a virtual-currency wallet known to be affiliated with fraudulent activity at the time of a transaction and identifying patterns that reflect money laundering or other illicit activity. The commissioner may request evidence from any virtual-currency kiosk operator of use of blockchain analytics.
2. A virtual-currency kiosk operator shall take reasonable steps to detect and prevent fraud, including establishing and maintaining a written antifraud policy. The antifraud policy must include:
  - a. The identification and assessment of fraud-related risk areas;
  - b. Procedures and controls to protect against identified risks;
  - c. Allocation of responsibility for monitoring risks; and
  - d. Procedures for the periodic evaluation and revision of the antifraud procedures, controls, and monitoring mechanisms.
3. Each virtual-currency kiosk operator shall designate and employ a compliance officer with the following requirements:
  - a. The individual must be qualified to coordinate and monitor compliance with this chapter and all other applicable federal and state laws and rules;
  - b. The individual must be employed full-time by the virtual-currency kiosk operator; and
  - c. The designated compliance officer may not be an individual who owns more than twenty percent of the virtual-currency kiosk operator by whom the individual is employed.
4. Compliance responsibilities required under federal and state laws and rules must be completed by full-time employees of the virtual-currency kiosk operator.

- 1        5. A virtual-currency kiosk operator shall maintain, implement, and enforce a written  
2        enhanced due diligence policy. The policy must be reviewed and approved by the  
3        virtual-currency kiosk operator's board of directors or equivalent governing body.  
4        6. A virtual-currency kiosk operator shall designate and employ a consumer protection  
5        officer. The consumer protection officer:  
6        a. Must be qualified to coordinate and monitor compliance with state and federal  
7        law;  
8        b. Must be employed full-time by the virtual-currency kiosk operator; and  
9        c. May not own more than twenty percent of the virtual-currency kiosk operator.

10       **SECTION 5.** Section 13-09.1-53 of the North Dakota Century Code is created and enacted  
11 as follows:

12       **13-09.1-53. Daily transaction limit.**

13       A virtual-currency kiosk operator may not accept transactions of more than two thousand  
14 dollars of cash or the equivalent in virtual currency per calendar day ~~for the first five~~  
15 ~~virtual-currency kiosk transactions occurring within the first thirty days of the first transaction~~  
16 with a single customer in this state via one or more virtual-currency kiosks operated by the  
17 same virtual-currency operator.

18       **SECTION 6.** Section 13-09.1-54 of the North Dakota Century Code is created and enacted  
19 as follows:

20       **13-09.1-54. Customer service.**

21       A virtual-currency kiosk operator performing business in this state shall provide live  
22 customer service at a minimum on Monday through Friday between eight a.m. central time and  
23 ten p.m. central time. The customer service toll-free number must be displayed on the  
24 virtual-currency kiosk or the virtual-currency kiosk screens.



*A Proud Past – A Promising Future*

# McLean County

STATE OF NORTH DAKOTA

Ladd R. Erickson  
McLean County State's Attorney

712 5<sup>th</sup> Avenue  
P.O. Box 1108  
Washburn, ND 58577-1108  
Phone: 701.462.8541  
Fax: 701.462.8212  
[www.mcleancountynd.gov](http://www.mcleancountynd.gov)  
Service: 28sa@nd.gov

Karissa K. Rittenbach, Legal Assistant  
[krittenbach@nd.gov](mailto:krittenbach@nd.gov); 701.462.8833  
Kelsey J. Renner, Legal Secretary  
[kjrenner@nd.gov](mailto:kjrenner@nd.gov); 701.462.8832

March 10, 2025

Mr. Chairman and members of the committee:

My name is Ladd Erickson and I am the McLean County State's attorney. I support HB1447, but would suggest the Committee revisit some amendments the House put into the original bill that inadvertently facilitates crypto currency scams instead of protecting people from them. Specifically, Section 5 of the engrossed bill, as I will explain in my oral testimony.



Pig butchering schemes often start with solicitations of modest investments intended to bolster your confidence. They usually involve some type of fake claim or falsified dashboard that shows assets exponentially growing, with the intent being to encourage larger and larger investments.

## A Slow Build

Here's how pig butchering investment schemes frequently work: A stranger will contact you out of the blue via text message, on social media or on a messaging application such as WhatsApp or WeChat and attempt to build rapport. They might provide an unusual explanation for why they're contacting you, such as having found your name in their contacts list, and often have online profiles that include fake but realistic-looking photos intended to pique your interest. They might also come across as wanting to develop a genuine friendship or romantic relationship.

Over the course of days, weeks or even months, the fraudster will send you messages about personal, non-investment-related topics. They might try to foster trust by sending pictures, talking about activities—such as volunteering—to demonstrate good character, or sharing fictitious life details that mirror your own. They might claim to be a widow, a single parent or even a member of the U.S. military living overseas, for example. In the process, the fraudster will also seek to obtain information that they can later use to manipulate you into surrendering your money.

Though these scams can present in different ways, inevitably the scammer will at some point steer the conversation toward investment-related topics, often asking whether you have an investment or crypto account.

## Sharpening the Knife

The goals for the next phase of the scheme are twofold: to create the perception that you'll make money by following the bad actor's instructions and to ensure that you have the ability to invest into the forthcoming scam.

In one common scenario, for example, a fraudster might share that they have a connection at a reputable financial institution who gives lucrative investment advice and offer to share that advice with you. They might send screenshots of their

alleged brokerage account to demonstrate investment gains from the connection's prior stock picks. After you express a willingness to invest, the bad actor might ask you to verify that your brokerage account has the ability to trade in the relevant security, then provide additional instructions, including the company to invest in, the specific quantity to purchase and a specific price. They'll typically claim that you need to place an order to buy the stock immediately and might also ask you to send a screenshot proving that you executed the trade.

In another common scenario, the bad actor will dangle riches supposedly made through trading cryptocurrency. After gaining your trust, they'll encourage you to purchase or transfer cryptocurrency assets using a specific trading platform, which is likely to be fake and controlled by the scammer or their associates.

Other variations of these scams have the same goal: Entice you to put your money toward the "opportunity" they've shared.

It's important to realize that, while you might be executing such trades in your own investment accounts and with your own funds, the fraudster might be manipulating your decision-making in these and other pig butchering scenarios.

## The Slaughter

Capitalizing on the relationship they've established with you, scammers will point to impressive gains from initial investments and urge you to deposit increasingly larger amounts. Once you do, however, the switch will flip, often leaving you facing devastating losses. The price of a stock that seemed poised to take off might rapidly plummet once the scammer's market manipulation kicks into high gear. Or the new crypto platform you recently moved your assets into might suddenly become inaccessible.

If you confront the bad actor regarding the losses, they might express empathy and offer to help you recover your money, perhaps attempting to persuade you to invest in another stock. They might cite additional taxes and fees that you must pay before withdrawing your funds, especially if the investment scam involved crypto assets. And sometimes the bad actor will ghost you once the investment goes south.





Bitcoin is 77,000 lines of computer code.

Vuk Martin



## BLOCKCHAIN

COLUMN A

COLUMN B

LADD

10 (Bitcoin)

Owner Applied  
Number  
Finish  
Condition  
Identifying Marks  
Recovered Date  
Owner  
Disposition  
Evidence Tag

Color Type      Color

Vehicle Type  
Vehicle Year  
Odometer  
Reading  
Body Style  
License Number  
License Exp. Date  
License State

Bicycle Make  
Bicycle Model  
Bicycle Speed  
Bicycle Wheel  
Size  
Color

Boat Name  
Boat Type  
HIN  
Hull Shape  
Propulsion  
Boat Length

Drug Type  
Drug Quantity  
Drug Measure

Notes

135.88 in charges from 6-4-  
2022 to 6-7-2022. Capital one  
card ending in # [REDACTED] belonging  
[REDACTED]

## Narrative

6/10/2022 12:00:00 AM

4427 - Matties, Aaron R

On this above date, I spoke with a [REDACTED] lives in Butte, North Dakota. [REDACTED] stated that last week in between May 31 and June 2nd that her computer locked-up and a number popped up on her screen to get it fixed. [REDACTED] stated that it was a "Microsoft Number" and that a phone number came up to call. The phone number 909-550-6296 was the number that was on her computer to call to fix the shutdown. [REDACTED] called the number and thought it was Microsoft. The person from "Microsoft" got some information from [REDACTED] entered a passcode into a box on her computer. This included where she banked at, and they stated that her accounts may have been hacked. [REDACTED] stated that they transferred her to Bremer Bank, Minneapolis, Minnesota and she spoke to Rick Harrison of Bremer Bank.

[REDACTED] stated that Mr. Harrison showed her columns on her computer, and that there was three columns, and there was writing and numbers in the columns. Mr. Harrison stated to her that those should be blank, and that there were scammers trying to get her money out of Bremer Bank. [REDACTED] was told that she needed to first remove her money from the bank, and get it secured into a different account. Mr. Harrison obtained her phone number from her and told her to go to the bank. Mr. Harrison gave her directions to Dakota Square Mall, to Crypto currency kiosk in Minot, North Dakota. Mr. Harrison informed her that what she needed to do was to put all of the money into a wallet. [REDACTED] stated that she received these "phone scans" on her phone from Mr. Harrison. She then deposited money using her driver's license into a dark web crypto currency account. She deposited money total of \$10,562 dollars on 06/02/2022. [REDACTED] then transferred \$5,059 into the same cryptocurrency kiosk on 6/3/2022. [REDACTED] bought "Litecoin" and "Dogecoin" during the transactions. There was also scan codes that I took pictures of. [REDACTED] kept telling me that



this is how she would keep her money safe from the scammers that hacked into her computer. [REDACTED] told me that her computer didn't work the next day, and was still locked up. [REDACTED] was told to continue to put more money into a Crypto Wallet to keep her money safe. [REDACTED] deposited more money into a Crypto Wallet on 6-7-2022 at a kiosk in Mandan, North Dakota. [REDACTED] deposited four deposits \$1600, 3700, 7,400, 300, into crpro currency wallets that Rick Harrison told her to put them in.

On 6-7-2022 I received a call from a Tad Pritchett of Morton County Sheriff's Department. Deputy Pritchett was in a store in Mandan, North Dakota Barney's 3.1 on 6th and Main Street, and workers told him about a lady that was shoving money into a crypto currency machine and was on the phone. Officer Pritchett stated to me that he talked to a lady named [REDACTED], and asked her if she was OK. [REDACTED] told the officer that she was helping her son [REDACTED] in California with investing money into crypto currency, and was on the phone with him. Officer Pritchett told me that he spoke with the person on the phone, who identified himself as [REDACTED], son of [REDACTED]. Officer [REDACTED] said that the man had an accent, and he asked [REDACTED] if her son had an accent. [REDACTED] stated that it was her son. I asked [REDACTED] about this when I took the report, and she stated that [REDACTED] told her to do this. I asked [REDACTED], didn't she think this was weird, and a scam, and she stated that it just didn't come to her at the moment. [REDACTED] went back home, and her computer was fixed.

[REDACTED] stated that she spoke with people personally at Bremer Bank in Minot, North Dakota. [REDACTED] was given information on scams, and received password protection on her accounts, and more security on her accounts. [REDACTED] stated to me that Bremer Bank checked and that they don't have a Rick Harrison working for them at any Bremer Bank. [REDACTED] had a total loss of \$28,621 for all her deposits to the Kiosks.

On 6-14-2022, I spoke with [REDACTED] about her Capital One Bank Account. [REDACTED] told me that she had charges that she didn't authorize to her Capital One Credit Card for \$135.88 total, and they were four different charges. Deputy Paul Barrette met with [REDACTED] at her residence in rural Butte, North Dakota, and provided picture copies of the account charges.

Charges were these:

6-03-2022-Probiller.com \$130.79  
06-03-2022-Probiller.com \$1.09  
6-6-2022-ecst.net\$2.00  
6-7-2022-vxnbill.com-\$2.00

[REDACTED] stated that her card was protected and she was credited with her money back on the account. I explained to [REDACTED] about her money, and about the "Dark Web." I told [REDACTED] that her money is from the crpto currency is so hard to trace and that she will not be able to get her money back. I told her to call Bremer Bank and ask them if she would have any account protection to get her money back. I gave [REDACTED] my card, and told her if she had any questions to call me.

End of Report, 4427

Please see Deputy Pritchett's report in sheriff's data

## Evidence Checklist

Additional Evidence Items?

Video Recording

In-Car Video

Surveillance

Interview Room

Other Recording

What other recordings are there?





March 10<sup>th</sup>, 2025

**Mr. Chairman and members of the Senate Industry and Business Committee:**

My name is Jacob Rued. I am Minot native and currently reside in rural Cass County.

For over the past decade, I have had the opportunity to serve our state in various law enforcement and private sector fraud prevention roles. I have proudly served our communities as a Cass County Deputy Sheriff, Fargo Police Officer, and Fargo Police Financial Crimes Detective. I currently work as a Fraud Investigator for the Minot-based community bank, First Western Bank. I hold certifications as a Certified Fraud Examiner by the Association of Certified Fraud Examiners and as a Certified Anti-Money Laundering and Fraud Professional by the American Bankers Association.

I give this testimony to you in **support of HB 1447** on behalf of myself, First Western Bank, and the North Dakota Banker's Association.

Unfortunately, my job must exist because of criminals who steal and defraud millions of dollars from North Dakotans using crypto kiosks, which scammers often deceptively refer to as "Federal Safety Lockers". In many cases I have investigated, our community members are indoctrinated, through fear, love, or greed, to withdraw their life savings in cash and deliver them to a crypto kiosk in their community or neighboring community. Once deposited, their funds are gone, unrecoverable, and certainly not in a "safety locker".

Our victims, often but not exclusively seniors, are rarely versed in understanding cryptocurrency or involved in legitimate investment with it. Their engagement with a crypto kiosk marks the first, last, and likely only cryptocurrency transaction they will ever complete. Their trust in the kiosk often based on the manipulated idea because the kiosk is "real" and physically present in their community, must mean any associated business is vetted and operated like a traditional ATM. *Why or how else would it be here?*

I believe HB 1447 strikes a reasonable balance in continuing to allow North Dakotans to engage with the plethora of legitimate, online crypto exchanges they may make deposits to via check, wire, and ACH while limiting a vulnerable population's exposure to a type of currency they are not familiar with. Specifically, HB 1447's requirement of receipted disclosures, operator fraud prevention requirements, physical receipts, and daily transaction limits are critical to its efficacy.

I offer you 2 further points to assist in your evaluation and decisioning on this bill.

1. First Western Bank operates in both Minnesota and North Dakota. In August of 2024, Minnesota enacted legislation similar HB 1447. The following is a contrast between 2 of my cases in these states to highlight pitfalls in the current total absence of our legislation and pitfalls of the enacted Minnesota legislation we should be wary of:
  - a. *North Dakota Resident* – young, newlywed couple (20s YOA). Husband is called and extorted to believe there is a warrant for his arrest. Husband withdraws \$15K from their bank account. Deposits all \$15K cash at a local crypto kiosk believing this will pay his government fines and prevent him from going to jail. Husband later realizes he was scammed. The couple is at 100% loss which is never recovered. The \$15K was a relatively considerable sum and intended to be used as a down payment on a house.
  - b. *Minnesota Resident* – elderly, retired widow. She is called by an FBI agent impersonator. The female is indoctrinated to believe her money is being stolen; she must withdraw all of her \$25K in savings in cash and take it to a Bitcoin ATM for safekeeping. The female is coached to lie to her bank and family about her withdrawal reason and is kept in fearful compliance by being ordered to have her phone listening in her pocket when inside the bank. The widow obtains her cash and goes to a nearby Crypto Kiosk at a gas station. The Widow registers as a new customer and is allowed by MN Law to deposit a \$2K maximum daily limit. Her scammer then instructs her to register 2 more times as 2 different people. Depositing \$2K a piece for a now total of \$6K. The widow returns home and the next day is sent back to the kiosk to register as a 3<sup>rd</sup> person and deposit another \$2K. The widow is enroute to deposit another \$2K as a 4<sup>th</sup> person when I contact and stop her. Had I not contacted her, in another 24 hours MN Law's daily \$2K limit would have expired for her, and she would have deposited everything that remained of her \$25K. MN law also compels crypto kiosk operators to refund victims of fraud in these scenarios, but because the widow only had a physical receipt for her first transaction, the kiosk operator refused to reimburse her for anything beyond the original \$2K. Because the widow had no ability to access the other virtual receipts in other people's names, she was told she had no evidence she'd done what she was claiming and would not be refunded.

# 2025 SENATE STANDING COMMITTEE MINUTES

## Industry and Business Committee Fort Union Room, State Capitol

HB 1447  
3/12/2025

A bill relating to virtual-currency kiosks.
---

2:56 p.m. Chairman Barta opened the hearing.

Members present: Chairman Barta, Vice-Chair Boehm, Senator Klein, Senator Kessel, Senator Enget

### Discussion Topics:

- Average fiscal amount per transaction
- Negotiation and decision timeframe
- Department of Financial Institutions and Bit Coin Depot
- Number of transactions
- Physical receipts and benefit
- Other states maximum daily limits
- Consumer risk and protection
- California's laws and regulations

3:03 p.m. Scott Meske, Bit Coin Depot, answered the committee's questions.

3:11 p.m. Lise Kruze, Commissioner, ND Department of Financial Institutions, answered the committee's questions.

3:18 p.m. Chairman Barta closed the hearing.

*Audrey Oswald, Committee Clerk*

# 2025 SENATE STANDING COMMITTEE MINUTES

## Industry and Business Committee Fort Union Room, State Capitol

HB 1447  
3/12/2025

A bill relating to virtual-currency kiosks.
---

3:32 p.m. Chairman Barta opened the hearing.

Members present: Chairman Barta, Vice-Chair Boehm, Senator Klein, Senator Kessel, Senator Enget

### Discussion Topics:

- Lowering daily transactional limits

3:33 p.m. Senator Klein moved to adopt amendment LC #25.1011.02001.

3:34 p.m. Senator Kessel seconded the motion.

Senators	Vote
Senator Jeff Barta	Y
Senator Keith Boehm	Y
Senator Mark Enget	Y
Senator Greg Kessel	Y
Senator Jerry Klein	Y

Motion passed 5-0-0.

3:36 p.m. Senator Klein moved a Do Pass As Amended.

3:36 p.m. Senator Enget seconded the motion.

Senators	Vote
Senator Jeff Barta	Y
Senator Keith Boehm	Y
Senator Mark Enget	Y
Senator Greg Kessel	Y
Senator Jerry Klein	Y

Motion passed 5-0-0.

Senator Barta will carry the bill.

3:37 p.m. Chairman Barta adjourned the meeting.

*Audrey Oswald, Committee Clerk*



Sixty-ninth  
Legislative Assembly  
of North Dakota

## PROPOSED AMENDMENTS TO FIRST ENGROSSMENT

### ENGROSSED HOUSE BILL NO. 1447

Introduced by

Representatives Swiontek, Christy, Hanson, Heinert, Schauer, J. Olson, Richter  
Senators Hogan, Klein, Lee, Rummel, Sickler

1 A BILL for an Act to create and enact sections 13-09.1-50, 13-09.1-51, 13-09.1-52, 13-09.1-53,  
2 and 13-09.1-54 of the North Dakota Century Code, relating to virtual-currency kiosks; and to  
3 amend and reenact section 13-09.1-44 of the North Dakota Century Code, relating to virtual-  
4 currency kiosks.

#### 5 BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

6 **SECTION 1. AMENDMENT.** Section 13-09.1-44 of the North Dakota Century Code is  
7 amended and reenacted as follows:

#### 8 **13-09.1-44. Definitions.**

9 For the purposes of sections 13-09.1-44 through ~~13-09.1-49~~ 13-09.1-54, the following  
10 definitions apply:

11 1. "Blockchain analytics" means the analysis of data from blockchains or publicly  
12 distributed ledgers, including associated transaction information.

13 ~~2. "Blockchain analytics software" means a software service that uses blockchain~~  
14 ~~analytics data to provide risk-specific information about virtual-currency~~  
15 ~~wallet transactions and virtual currency addresses.~~

16 3.2. "Control of virtual currency", when used in reference to a transaction or relationship  
17 involving virtual currency, means the power to execute unilaterally or prevent  
18 indefinitely a virtual-currency transaction.

19 2.4.3. "Exchange", used as a verb, means to assume control of virtual currency from or on  
20 behalf of a person, at least momentarily, to sell, trade, or convert:

- 1 a. Virtual currency for money, bank credit, or one or more forms of virtual currency;
- 2 or
- 3 b. Money or bank credit for one or more forms of virtual currency.

4 5.4. "Transaction hash" means a unique identifier made up of a string of characters that act  
5 as a record and provide proof the transaction was verified and added to the  
6 blockchain.

7 3.6.5. "Transfer" means to assume control of virtual currency from or on behalf of a person  
8 and to:

- 9 a. Credit the virtual currency to the account of another person;
- 10 b. Move the virtual currency from one account of a person to another account of the  
11 same person; or
- 12 c. Relinquish control of virtual currency to another person.

13 4.7.6. "United States dollar equivalent of virtual currency" means the equivalent value of a  
14 particular virtual currency in United States dollars shown on a virtual-currency  
15 exchange based in the United States for a particular date or period specified in this  
16 chapter.

17 5.8.7. "Virtual currency":

- 18 a. Means a digital representation of value that:
  - 19 (1) Is used as a medium of exchange, unit of account, or store of value; and
  - 20 (2) Is not money, whether or not denominated in money; and
- 21 b. Does not include:
  - 22 (1) A transaction in which a merchant grants, as part of an affinity or rewards  
23 program, value that cannot be taken from or exchanged with the merchant  
24 for money, bank credit, or virtual currency; or
  - 25 (2) A digital representation of value issued by or on behalf of a publisher and  
26 used solely within an online game, game platform, or family of games sold  
27 by the same publisher or offered on the same game platform.

28 9.8. "Virtual-currency address" means an alphanumeric identifier associated with a  
29 virtual-currency wallet identifying the location to which a virtual-currency transaction  
30 may be sent.

1 ~~6.10.9.~~ "Virtual-currency administration" means issuing virtual currency with the authority to  
2 redeem the currency for money, bank credit, or other virtual currency.

3 ~~7.11.10.~~ "Virtual-currency business activity" means:

- 4 a. Exchanging, transferring, or storing virtual currency or engaging in virtual-  
5 currency administration, whether directly or through an agreement with a virtual-  
6 currency control-services vendor;
- 7 b. Holding electronic precious metals or electronic certificates representing interests  
8 in precious metals on behalf of another person or issuing shares or electronic  
9 certificates representing interests in precious metals; or
- 10 c. Exchanging one or more digital representations of value used within one or more  
11 online games, game platforms, or family of games for:
- 12 (1) Virtual currency offered by or on behalf of the same publisher from which  
13 the original digital representation of value was received; or
- 14 (2) Money or bank credit outside the online game, game platform, or family of  
15 games offered by or on behalf of the same publisher from which the original  
16 digital representation of value was received.

17 ~~8.12.11.~~ "Virtual-currency control-services vendor" means a person that has control of virtual  
18 currency solely under an agreement with a person that, on behalf of another person,  
19 assumes control of virtual currency.

20 ~~13.12.~~ "Virtual-currency kiosk" means an electronic terminal acting as a mechanical agent of  
21 the virtual-currency kiosk operator to enable the virtual-currency kiosk operator to  
22 facilitate the exchange of virtual currency for money, bank credit, or other virtual  
23 currency, including by:

- 24 a. Connecting directly to a separate virtual-currency exchange that performs the  
25 actual virtual-currency transmission; or
- 26 b. Drawing upon the virtual currency in the possession of the electronic terminal's  
27 operator.

28 ~~14.13.~~ "Virtual-currency kiosk operator" means a person that ~~engages in virtual-currency~~  
29 ~~business activity via a money transmission kiosk located in this state or a person that~~  
30 ~~owns, operates, or manages a money transmission kiosk located in this state through~~



1 ~~which virtual-currency business activity is offered~~ operates a virtual currency kiosk in  
2 this state.

3 ~~15-14.~~ "Virtual-currency kiosk transaction" means:

4 a. A transaction conducted or performed, in whole or in part, by electronic means  
5 via a virtual-currency kiosk.

6 b. A transaction made at a virtual-currency kiosk to purchase virtual currency with  
7 fiat currency or to sell virtual currency for fiat currency.

8 ~~16-15.~~ "Virtual-currency wallet" means a software application or other mechanism providing a  
9 means to hold, store, or transfer virtual currency.

10 **SECTION 2.** Section 13-09.1-50 of the North Dakota Century Code is created and enacted  
11 as follows:

12 **13-09.1-50. Virtual-currency kiosks.**

13 1. A kiosk operator may not engage in virtual-currency business activity or hold itself out  
14 as being able to engage in virtual-currency business activity with or on behalf of  
15 another person unless the kiosk operator is licensed in this state as a money  
16 transmitter.

17 2. A virtual-currency kiosk operator shall comply with all requirements of a money  
18 transmitter under this chapter.

19 3. A virtual-currency kiosk operator may not locate, or allow a third party to locate, a  
20 virtual-currency kiosk in this state unless the virtual-currency kiosk:

21 a. Is placed in a commercially accessible area;

22 b. Is accessible to users with sufficient space to account for mobility limitations of  
23 users; and

24 c. Is subject to security features, including sufficient lighting and surveillance.

25 4. Each virtual-currency kiosk operator shall submit a quarterly report of the location of  
26 each virtual-currency kiosk located within the state to the commissioner within  
27 forty-five days of the end of the calendar quarter. The location report must include:

28 a. The company's legal name;

29 b. Any fictitious or trade name;

30 c. The physical address;

31 d. The start date of operation of the virtual-currency kiosk at the location;



- 1 e. The end date of operation of the virtual-currency kiosk at the location, if
- 2 applicable; and
- 3 f. The virtual-currency addresses associated with the virtual-currency kiosk.

4 **SECTION 3.** Section 13-09.1-51 of the North Dakota Century Code is created and enacted  
5 as follows:

6 **13-09.1-51. Disclosures.**

- 7 1. A virtual-currency kiosk operator shall disclose in a clear, conspicuous, and easily
- 8 readable manner in the chosen language of the customer, all relevant terms and
- 9 conditions generally associated with the products, services, and activities of the
- 10 virtual-currency kiosk operator and virtual currency.
- 11 2. The virtual-currency kiosk operator must receive acknowledgment of receipt of all
- 12 disclosures required under this section via confirmation of consent.
- 13 3. Each virtual-currency kiosk must include a warning written prominently and in bold
- 14 type, stated in substantially the following form:
- 15 a. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A
- 16 STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND
- 17 THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:
- 18 (1) Claims of a frozen bank account or credit card.
- 19 (2) Fraudulent bank transactions.
- 20 (3) Claims of identity theft or job offerings in exchange for payments.
- 21 (4) Requests for payments to government agencies or companies.
- 22 (5) Requests for disaster relief donations or loans.
- 23 (6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for
- 24 vehicles.
- 25 (7) Prompts to click on desktop popups, such as virus warnings or
- 26 communication from alleged familiar merchants.
- 27 (8) Communication from someone impersonating a representative of your bank
- 28 or a law enforcement officer.
- 29 (9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW
- 30 ENFORCEMENT OFFICER BEFORE ANY TRANSACTION.

- 1           b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE  
2           RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS  
3           VIRTUAL-CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE  
4           RISKS AND WISH TO CONTINUE WITH CONDUCTING MY  
5           VIRTUAL-CURRENCY KIOSK TRANSACTION. PROTECT YOURSELF FROM  
6           FRAUD. NEVER SEND MONEY TO SOMEONE YOU DO NOT KNOW.
- 7       4. The commissioner shall require the disclosure of material risks associated with virtual  
8       currency and virtual-currency transactions, including:
- 9           a. The transaction may not be reversed;  
10          b. The virtual-currency kiosk operator's liability for unauthorized virtual currency  
11          transactions;  
12          c. The virtual-currency kiosk customer's liability for unauthorized currency  
13          transactions;  
14          d. Virtual currency is not legal tender, backed or insured by the government, and  
15          accounts and value balances are not subject to federal deposit insurance  
16          corporation, national credit union administration, or securities investor protection  
17          corporation protections;  
18          e. Some virtual currency transactions are deemed to be made when recorded on a  
19          public ledger which may not be the date or time when the individual initiates the  
20          transaction;  
21          f. Virtual currency's value may be derived from market participants' continued  
22          willingness to exchange fiat currency for virtual currency, which may result in the  
23          permanent and total loss of a particular virtual currency's value if the market for  
24          virtual currency disappears;  
25          g. An individual who accepts a virtual currency as payment today is not required to  
26          accept and might not accept virtual currency in the future;  
27          h. The volatility and unpredictability of the price of virtual currency relative to fiat  
28          currency may result in a significant loss over a short period;  
29          i. The nature of virtual currency means any technological difficulties experienced by  
30          virtual-currency kiosk operators may prevent access to or use of an individual's  
31          virtual currency; and

- 1           j. Any bond maintained by the virtual-currency kiosk operator for the benefit of an  
2           individual may not cover all losses an individual incurs.
- 3       5. The commissioner shall require disclosure of:
- 4           a. The amount of the transaction denominated in United States dollars as well as  
5           the applicable virtual currency.
- 6           b. Any fees or expenses charged by the virtual-currency kiosk operator.
- 7           c. Any applicable exchange rates.
- 8           d. A daily virtual-currency transaction limit of no more than two thousand dollars ~~for~~  
9           ~~the first five transactions within the first thirty day period~~ per day.
- 10          e. Notice of a change in the virtual-currency kiosk operator's rules or policies.
- 11          f. The name, address, and telephone number of the owner of the kiosk and the  
12          days, time, and means by which a consumer may contact the owner for  
13          consumer assistance. Any relevant state and local law enforcement agency for  
14          reporting fraud must be displayed on or at the location of the virtual-currency  
15          kiosk or on the first screen of the kiosk.
- 16          g. Under what circumstances the virtual-currency kiosk operator, without a court or  
17          government order, discloses a person's account information to third parties.
- 18          h. Other disclosures customarily given in connection with a virtual currency  
19          transaction.
- 20       6. After the completion of each transaction, the virtual-currency kiosk operator shall  
21       provide an individual with a choice of a physical or digital receipt secured with  
22       two-factor identification in the language chosen by the customer containing the  
23       following:
- 24           a. The virtual-currency kiosk operator's name and contact information, including a  
25           telephone number to answer questions and register complaints;
- 26           b. The relevant state and local law enforcement or government agency for reporting  
27           fraud;
- 28           c. The type, value, date, and precise time of the transaction, transaction hash, and  
29           each applicable virtual-currency address;
- 30           d. A unique transaction number able to be linked to the sender during a fraud  
31           investigation;



- 1 e. A unique transaction number able to be linked to the designated recipient during
- 2 a fraud investigation;
- 3 f. All fees charged;
- 4 g. The exchange rate of the virtual currency to United States dollars;
- 5 h. A statement of the virtual-currency kiosk operator's liability for nondelivery or
- 6 delayed delivery; and
- 7 i. A statement of the virtual-currency kiosk operator's refund policy.

8 **SECTION 4.** Section 13-09.1-52 of the North Dakota Century Code is created and enacted  
9 as follows:

10 **13-09.1-52. Prevention of fraudulent activity.**

- 11 1. A virtual-currency kiosk operator shall use blockchain analytics software to assist in
- 12 the detection and prevention of suspicious activity, including sending purchased virtual
- 13 currency from a virtual-currency kiosk operator to a virtual-currency wallet known to be
- 14 affiliated with fraudulent activity at the time of a transaction and identifying patterns
- 15 that reflect money laundering or other illicit activity. The commissioner may request
- 16 evidence from any virtual-currency kiosk operator of use of blockchain analytics.
- 17 2. A virtual-currency kiosk operator shall take reasonable steps to detect and prevent
- 18 fraud, including establishing and maintaining a written antifraud policy. The antifraud
- 19 policy must include:
  - 20 a. The identification and assessment of fraud-related risk areas;
  - 21 b. Procedures and controls to protect against identified risks;
  - 22 c. Allocation of responsibility for monitoring risks; and
  - 23 d. Procedures for the periodic evaluation and revision of the antifraud procedures,
  - 24 controls, and monitoring mechanisms.
- 25 3. Each virtual-currency kiosk operator shall designate and employ a compliance officer
- 26 with the following requirements:
  - 27 a. The individual must be qualified to coordinate and monitor compliance with this
  - 28 chapter and all other applicable federal and state laws and rules;
  - 29 b. The individual must be employed full-time by the virtual-currency kiosk operator;
  - 30 and



- 1           c. The designated compliance officer may not be an individual who owns more than  
2           twenty percent of the virtual-currency kiosk operator by whom the individual is  
3           employed.
- 4           4. Compliance responsibilities required under federal and state laws and rules must be  
5           completed by full-time employees of the virtual-currency kiosk operator.
- 6           5. A virtual-currency kiosk operator shall maintain, implement, and enforce a written  
7           enhanced due diligence policy. The policy must be reviewed and approved by the  
8           virtual-currency kiosk operator's board of directors or equivalent governing body.
- 9           6. A virtual-currency kiosk operator shall designate and employ a consumer protection  
10          officer. The consumer protection officer:
  - 11          a. Must be qualified to coordinate and monitor compliance with state and federal  
12          law;
  - 13          b. Must be employed full-time by the virtual-currency kiosk operator; and
  - 14          c. May not own more than twenty percent of the virtual-currency kiosk operator.

15          **SECTION 5.** Section 13-09.1-53 of the North Dakota Century Code is created and enacted  
16 as follows:

17          **13-09.1-53. Daily transaction limit.**

18          A virtual-currency kiosk operator may not accept transactions of more than two thousand  
19          dollars of cash or the equivalent in virtual currency per calendar day for the first five  
20          ~~virtual-currency kiosk transactions occurring within the first thirty days of the first transaction~~  
21          with a single customer in this state via one or more virtual-currency kiosks operated by the  
22          same virtual-currency operator.

23          **SECTION 6.** Section 13-09.1-54 of the North Dakota Century Code is created and enacted  
24 as follows:

25          **13-09.1-54. Customer service.**

26          A virtual-currency kiosk operator performing business in this state shall provide live  
27          customer service at a minimum on Monday through Friday between eight a.m. central time and  
28          ten p.m. central time. The customer service toll-free number must be displayed on the  
29          virtual-currency kiosk or the virtual-currency kiosk screens.

**REPORT OF STANDING COMMITTEE  
ENGROSSED HB 1447**

**Industry and Business Committee (Sen. Barta, Chairman)** recommends **AMENDMENTS** ([25.1011.02001](#)) and when so amended, recommends **DO PASS** (5 YEAS, 0 NAYS, 0 ABSENT OR EXCUSED AND NOT VOTING). HB 1447 was placed on the Sixth order on the calendar. This bill does not affect workforce development.