# NDBA Live
## November 4, 2026

Topics Covered:

- Member Questions
- 2027 Legislative Priorities
- North Korea Responsible for $6 Billion + Binance Hack
- OCC GENIUS Act Final Rule Effective January 18, 2027
- OCC Debanking Report
- Bank of America BSA/AML Enforcement
- When Your Customer Gives AI the Keys to Their Bank Account – Who Is Responsible?
- AntiTrust Compliance Reminder
- Upcoming Events

DISCLAIMER: THESE MATERIALS PROVIDE GENERAL INFORMATION AND ARE INTENDED FOR EDUCATIONAL PURPOSES ONLY. THESE MATERIALS DO NOT PROVIDE, NOR ARE THEY INTENDED TO SUBSTITUTE FOR, LEGAL ADVICE.

## Member Questions

**Question 1:** Our bank was presented with an Affidavit for Collection of Personal Property from a funeral home director. They also provided the bill for the funeral of the client that the family never paid and are asking to claim the amount owed.

We have not run into this and I couldn't find any guidance in Century Code or law. This seems like a valid request to pay the amount owed to the funeral home, but I didn't know if there was any law preventing and making sure we should take no other considerations or proof before paying out.

**Response:** **I'm unsure how a creditor like a funeral home could be considered a "successor of the decedent" as required under Chapter 30.1-23 of the North Dakota Century Code.**

**I don't think a funeral home does qualify and therefore you might want to run it by the bank's counsel.**

---

**Question 2:** We are reaching out for some guidance on an altered check one of our customers had clear their account. I did determine that it was in fact an altered check not a counterfeit, and I sent the bank of first deposit an altered check warranty claim letter via certified mail. From my research, it appears that the bank of first deposit is liable for altered checks in most cases. Is this correct?

Recently, the bank of first deposit said it was denied and we should be receiving a letter on next steps. If they do not follow through on their end, what are our options? Are we liable to credit the customer back? The customer did notify us within the time frame that is spelled out on our account disclosure.

**Response:** **"A bank may charge against the account of a customer an item which is properly payable from that account…An item is properly payable if it is authorized by the customer and complies with any agreement between the customer and the bank." N.D.C.C. § 41-04-32 (U.C.C. § 4-401). There are exceptions to this general strict liability, such as when the customer does not timely report an unauthorized signature or alteration under N.D.C.C. § 41-04-37 (U.C.C. § 4-406).**

**For altered checks, the bank may generally recover the amount from the depositary bank pursuant to a breach of warranty claim. *See* N.D.C.C. §§ 41-04-19 (U.C.C. § 4-207), 41-04-20 (U.C.C. § 4-208).**

**An action to enforce a breach of warranty claim must be commenced within 3 years after the cause of action accrues. *See* N.D.C.C. § 41-04-11 (U.C.C. § 4-111).**

**In accordance with the foregoing, yes, banks are generally liable to refund their customers (especially if reported timely). The bank is also able to recover such amounts from the depository bank through a breach of warranty claim. When a depository bank denies a breach of warranty claim, the claimant should generally discuss next steps with legal counsel. It is noted that a lawsuit would need to be commenced within 3 years.**

---

**Question 3:** Can banks prohibit customers and/or employees from wearing Meta glasses?

**Response:** **Smart glasses (i.e., Ray-Ban Meta, Google Glass or similar devices) are wearable devices capable of recording video and audio, taking photographs, and transmitting information. While I cannot provide legal advice, the following are legal considerations that may relate to the use of smart glasses on bank premises:**

**Confidentiality and Safeguarding of Customer Information**

**Under Chapter 6-08.1 of the North Dakota Century Code, banks generally may not disclose customer information except as authorized by statute. "Customer information" is broadly defined to include any records held by a financial institution pertaining to a customer's relationship with the financial institution, as well as any information derived from such records. *See* N.D.C.C. § 6-08.1-01(2).**

**Additionally, the Gramm-Leach-Bliley Act (GLBA) requires banks to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information. *See* 15**

**U.S.C. § 6801(a). As part of that, banks must develop, implement, and maintain a written comprehensive information security program containing administrative, technical and physical safeguards that are appropriate to its size and complexity, activities and the sensitivity of the customer information involved. *See* 12 C.F.R. Appendix B to Part 364 – Interagency Guidelines Establishing Information Security Standards. The program must ensure the security and confidentiality of customer information, protect against anticipated threats or hazards, and prevent against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. *See id.* The bank must implement access controls to authenticate and permit access only to authorized users and limit an authorized user's access to customer information needed for the user's duties and functions. *See id.***

**Recording Laws**

**In North Dakota, the interception of wire or oral communications is generally prohibited, subject to certain exceptions. *See* N.D.C.C. § 12.1-15-02. "Intercept" means the aural acquisition of the contents of any wire or oral communication through the use of an electronic, mechanical, or other device, or by secretly overhearing the communication. N.D.C.C. § 12.1-15-04. One exception to the general prohibition applies when the person is a party to the communication or one of the parties to the communication has given prior consent, provided such communication is not intercepted for the purpose of committing a crime or other unlawful harm. *See* N.D.C.C. § 12.1-15-02. Accordingly, a person wearing smart glasses may be able to record a conversation without the knowledge or consent of the other participants if the person is a party to the communication, subject to the statutory limitations.**

**Section 13-01.1-01-14 of the North Dakota Administrative Code also expressly prohibits the recording of meetings and conversations involving the commissioner or the department staff discussing examination facts, reports, or other records created by the commissioner or the department without the prior approval of the commissioner (except as allowed by the open meeting laws).**

**ADA**

**The Americans with Disabilities Act (ADA) generally requires employers to provide reasonable accommodations to qualified individuals with disabilities, absent undue hardship. 42 U.S.C. § 12112. *See also* N.D.C.C. § 14-02.4-03(2) ("It is a discriminatory practice for an employer to fail or refuse to make reasonable accommodations for an otherwise qualified individual...An employer is not required to provide an accommodation that would disrupt or interfere with the employer's normal business operations; threaten an**

**individual's health or safety; contradict a business necessity of the employer; or impose an undue hardship on the employer...")**

**For customers, banks are generally considered places of public accommodation under the ADA. *See* 42 U.S.C. § 12181(7)(F). A place of public accommodation may be required to make reasonable modifications to its policies when necessary to provide an individual with a disability access to its goods and services. See 42 U.S.C. § 12182(b)(2)(A)(ii).**

**Accordingly, a smart-glasses prohibition may raise ADA considerations if the employee or customer requests to use the device as an accommodation for a disability.**

**Protected Concerted Activity**

**Section 7 of the National Labor Relations Act (NLRA) guarantees employees the right to engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection. 29 U.S.C. § 157. It is an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of such guaranteed rights. *See* 29 U.S.C. § 158. North Dakota has a similar statutes. *See* N.D.C.C. § 34-12-02 ("Employees have the right to…engage in…lawful concerted activities for the purpose of collective bargaining or other mutual aid or protection…"); N.D.C.C. § 34-12-03 (stating it is an unfair labor practice for any employer to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 34-12-02).**

**In *Whole Foods Mkt. Grp., Inc. v. NLRB*, the Second Circuit Court of Appeals affirmed the NLRB's determination that Whole Foods violated the NLRA by broadly prohibiting all recording without management approval. *See*, 691 Fed. Appx. 49, 51 (2nd Cir. 2017). The court expressly noted that not every no-recording policy violates the NLRA. *See id.* (citing *Flagstaff Med. Ctr., Inc.*, 357 N.L.R.B. 659, 659-60, 683 (2011) (holding that no-photography policy was lawful where hospital demonstrated patient privacy interest)).**

---

## 2027 Legislative Priorities

Fraud is a key priority for the upcoming North Dakota legislative session. As scams and fraudulent activity continue to evolve, legislation is being developed to address emerging methods of fraud, protect consumers, and hold individuals and entities accountable for facilitating unlawful activity. NDBA is focused on the following areas:

- **Cryptokiosks –** Prohibit virtual-currency kiosks.
- **Fraudulent Social Media Advertising –** Establish responsibilities for social media platforms to identify, vet, and remove fraudulent advertisements appearing on their platforms.

- **Telecommunications Fraud –** Establish responsibilities for telecommunications providers to address the use of their networks to facilitate fraudulent activity.
- **Mail Receptacle Security and Protection –** Establish specific criminal penalties for the unauthorized access, theft, reproduction or use of mail receptable access devices, including mailbox keys and other devices used to access mail receptacles.

On the federal level, NDBA supports:

- **GUARD Act** – The Guarding Unprotected Aging Retirees from Deception (GUARD) Act, cosponsored by Congresswoman Julie Fedorchak, passed the U.S. House of Representatives in September 2026. The legislation would give state, local, and tribal law enforcement agencies greater flexibility to use existing federal grant funding to investigate financial fraud, elder financial exploitation, and cryptocurrency investment scams. It would also expand access to federal blockchain-tracing resources to help law enforcement investigate and track stolen funds. The bill has advanced to the Senate for consideration.
- **SCAM Act** - The Safeguarding Consumers from Advertising Misconduct (SCAM) Act seeks to reduce fraudulent and deceptive online advertising by requiring platforms to verify advertisers, implement fraud detection measures, and establish procedures for investigating and removing fraudulent advertisements. NDBA will be advocating for passage of the SCAM Act as part of our continued efforts to combat online fraud.

---

## North Korea Responsible for $6 Billion + Binance Hack

The FBI has announced that North Korea was responsible for stealing more than $6 billion in virtual assets from Binance, the world's largest cryptocurrency exchange. The FBI identified the activity as "TraderTraitor," a North Korean state-sponsored cyber operation. Working with the U.S. Secret Service and IRS Criminal Investigation, the FBI observed the hackers converting the stolen assets primarily into Ethereum. Authorities anticipate that the stolen assets will be further laundered through decentralized finance (DeFi) platforms and instant cryptocurrency exchange services to conceal their origins and facilitate additional transfers. The FBI, U.S. Secret Service, and IRS are urging cryptocurrency service providers, including exchange operators, DeFi services, blockchain analytics firms, and other virtual asset providers, to identify and block transactions involving wallet addresses associated with the hackers. The FBI published a list of identified cryptocurrency wallet addresses connected to the theft to assist in those efforts and is requesting that individuals with relevant information contact their local FBI field office or submit a report to the Internet Crime Complaint Center.

---

## OCC GENIUS Act Final Rule Effective January 18, 2027

On October 21, 2026, the Office of the Comptroller of the Currency (OCC) issued a final rule to implement the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act regarding the issuance of payment stablecoins and certain related activities by entities subject to the OCC's jurisdiction.

The final rule will be applicable to national banks and their subsidiaries, federal savings associations and their subsidiaries, federal branches and their subsidiaries, foreign payment stablecoin issuers, nonbank entities that seek to be or are approved as federal qualified payment stablecoin issuers, and state qualified payment stablecoin issuers for whom the OCC has regulatory or enforcement authority pursuant to the GENIUS Act.

The final rule will be effective on January 18, 2027.

Link: https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-50.html

---

## OCC Debanking Report

On October 14, 2026, the OCC reported supervisory findings concerning debanking activities at the nine largest national banks it supervises. The OCC's report shows that all nine banks had policies or practices that required, encouraged, or otherwise influenced banks to deny or limit access to financial services to Americans because of their political or religious beliefs or lawful business activities.

Link: https://www.occ.gov/news-issuances/news-releases/2026/nr-occ-2026-90.html

---

## Bank of America BSA/AML Enforcement

On October 13, 2026, the U.S. Department of the Treasury announced enforcement actions imposing more than $1.21 billion in penalties against Bank of America for violations of anti-money laundering and sanctions laws. The Financial Crimes Enforcement Network (FinCEN) assessed a $1.2 billion penalty for the bank's failure to mitigate and report priority national security risks; the OCC assessed a $750 million civil money penalty for the bank's deficient and ineffective BSA/AML compliance program; and the Office of Foreign Assets Control (OFAC) announced an $11.6 million settlement with the bank for its violations of numerous sanctions programs.

Link: https://home.treasury.gov/news/press-releases/sb0657

---

## When Your Customer Gives AI the Keys to Their Bank Account—Who Is Responsible?

Artificial intelligence is creating a new challenge for banks: What happens when a customer gives an AI agent access to their bank accounts?

In a recent incident reported by *The Wall Street Journal*, a technology executive created an AI agent called "Personal CFO" and gave it access to his checking and savings accounts. The agent was supposed to monitor his finances but instead mistakenly shared sensitive banking information in a company Slack channel. No funds were reportedly stolen, but the incident highlights a growing concern.

Now imagine a customer authorizing an AI agent to pay bills, transfer funds, and manage cash flow. The agent initiates a $75,000 transfer that the customer claims was never authorized.

**Who bears the loss—the customer, the bank, or the AI provider?**

The answer raises significant legal questions under Regulation E, UCC Article 4A, and traditional principles of agency and authority. Does giving an AI agent access to online banking credentials authorize its transactions? What if the agent exceeds its instructions or is manipulated by a third party?

**The Bottom Line**: As AI agents become more sophisticated, banks should review their electronic banking agreements, security procedures, and policies governing third-party access. The technology is moving quickly, and banks should address these risks before the first disputed AI-initiated transfer arrives.

---

## ANTITRUST COMPLIANCE REMINDER

The North Dakota Bankers Association ("NDBA") is committed to full compliance with applicable federal and state antitrust laws. These laws preserve fair competition and prohibit agreements or coordinated conduct among competitors that unlawfully restrain trade. Because member institutions may compete, all participants in NDBA meetings, committees, conferences, peer groups, and other activities must observe antitrust requirements.

### PROHIBITED DISCUSSIONS AND ACTIVITIES

**Pricing and rates:** Current or future interest rates, loan pricing, deposit rates, fees, service charges, or other competitive pricing terms.

**Markets and customers:** Agreements to allocate customers, geographic markets, products, or business opportunities.

**Business strategies:** Confidential future competitive plans, lending or deposit strategies, or other competitively sensitive decisions.

**Boycotts and refusals to deal:** Agreements to collectively refuse business with customers, vendors, competitors, or other parties.

**Employment practices:** Agreements on compensation, recruitment, hiring, or other competitive employment terms.

### PERMITTED ASSOCIATION ACTIVITIES

Members may discuss legislation, regulation, industry developments, compliance, education, and other legitimate association matters. Surveys, benchmarking, and information sharing must be structured to avoid improper disclosure of competitively sensitive information. Each institution must independently determine its pricing, strategies, employment practices, and other competitive decisions.

**MEETING PROCEDURES**

Stay within the agenda and legitimate association purposes.

Do not share confidential or competitively sensitive business information.

If a discussion raises antitrust concerns, note your concerns, take a break, and notify NDBA leadership or legal counsel.

---

## Upcoming Events

NDBA has many exciting and informational events planned. Below are some special dates to mark on your calendars!

- **Bank Management Conference & Legislative Reception |** January 2027 | Bismarck
- **2027 Tri-State Trust Conference |** April 2027 | Fargo
- **2027 SDBA/NDBA Annual Convention |** June 6-8, 2027 | Sioux Falls, SD