NDBA Live
July 8, 2026

Topics Covered:

Member Questions

Question 1: Can you run a ChexSystem on authorized signers without their permission?

Response: **First, I suggest taking a look at your deposit account agreement to see if it authorizes credit checks for all account signatories. And if it does allow for it then you can follow the contractual language but to be safe you may choose to run a identification verification check for the authorized signor and just not pull a "hard search" tied to credit.**

Note that the Fair Credit Reporting Act and your Deposit account agreement will govern when, if and what types of credit searches can be performed.

Fair Credit Reporting Act | Federal Trade Commission

Question 2: How would it best be handled for when/if when an insurance agency accepts checks written out to the agency themselves or to the underwriting company and deposits them at the bank in the agencies name? For example, ABC Agency has an account at bank and checks are written out to Progressive Insurance let's say. I believe most agencies then deposit the check(s) and pay the underwriters themselves as a convenience to their customers. If this presents some risks, what can we do to mitigate this? Are there ND laws to consider? What are other banks doing?

Response: **My concern is that the Agency depositing the checks without "progressive's" endorsement might violate presentment and transfer warranties under Articles 3 and 4 of the Uniform Commercial Code but I also wonder if the Insurance Agency's agreement with the insurance companies contain a limited power of attorney that would allow the Agency to deposit checks on its behalf.**

Question 3: Customer has two POAs (aunt and brother-in-law). The aunt filed for guardianship and the Customer is considered incapacitated. The brother-in-law is farming the land for Customer this year. The aunt is wondering if the brother-in-law is able to write checks on behalf of the individual for farm expenses. The brother-in-law is POA on the account, but does the POA no longer exist since there is now a court appointed guardian? If it does, is the aunt able to add the brother-in-law to the account as a joint owner/signer?

Also, the guardianship is set to expire August 5, 2026. I am guessing the guardianship will be extended by the aunt, but if not, are the POAs effective again if they are considered voided by the appointment of a guardian?

Response: **I cannot give you direct legal advice but I can tell you that generally the Order Appointing the Conservator will state whether previous POA's have been revoked and that a Court appointed Conservator has the right to act on behalf of the individual as given by the Court. In this case it looks like the Conservator would have the authority to revoke a previous POA if she chose to do so.**

I would request a signed statement from the Conservator telling your Bank if the other POA is still valid and enforceable.

I would not offer any legal advice or interpretation of the rights and limitations of the POA or Conservatorship to the Conservator and let her know if she has questions she will need to speak with a lawyer, presumably the one that assisted in getting the Order for Conservatorship.

Question 4: Bank loaned money to John Doe, and John Doe granted Bank a security interest in vehicles. Bank is named as a lienholder on a Certificate of Title which lists two individuals as owners (e.g., "John Doe or Jane Roe"). Jane Roe is not a party to any of the loan documents. The estate claims Jane Roe has no interest in the vehicle because she is not on the loan documents – is that accurate?

Response: **With respect to Jane Roe's ownership interest, the fact that she is not a party to the loan documents does not, by itself, determine whether she has an ownership interest in the vehicle.**

Under North Dakota law, the ownership of property by several persons is either: (1) of joint interests; (2) of partnership interests; or (3) of interests in common. N.D.C.C. § 47-02-05. "A joint interest is one owned by several persons in equal share by a title created by a single will or transfer, when expressly declared in the will or transfer to be a joint tenancy, or when granted or devised to executors or trustees as joint tenants." N.D.C.C. § 47-02-06. "A partnership interest is one owned by several persons in partnership for partnership purposes." N.D.C.C. § 47-02-07. "An interest in common is one owned by several persons not in joint ownership or partnership. Every interest created in favor of several persons in their own right is an interest in common, unless acquired by them in partnership for partnership purposes, or unless declared in its creation to be a joint tenancy." N.D.C.C. § 47-02-08.

The ability of an owner to convey or encumber the other owner's interest in property, and the ownership of the property after death of one owner, depends on the type of concurrent ownership.

Here, John Doe's estate may have a claim to the vehicle and Jane Roe may have a claim to the vehicle. The bank should consult with legal counsel regarding the enforceability of its security interest and the respective rights of the parties.

2026 NDBA Leadership

The North Dakota Bankers Association's 2026 leadership team continues under its elected Executive Officers, providing guidance for the year ahead. The officers include Jamie Nelson (TruCommunity Bank) as Chair, Duane Bowman (Dakota Western Bank) as Vice Chair, and Paige Bjornson (Dacotah Bank) as Treasurer. Together, they will help direct the Association's advocacy, education, and industry engagement efforts, supporting NDBA's ongoing mission of advancing North Dakota's banking industry.

Regulators Propose BSA Compliance Rules for Stablecoin Issuers Under GENIUS Act

On June 18, 2026 the Financial Crimes Enforcement Network (FinCEN), together with the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA), issued a joint proposed rule to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act).

The proposed rule would formally treat permitted payment stablecoin issuers as financial institutions under the Bank Secrecy Act (BSA). This designation would require issuers to establish and maintain effective customer identification programs (CIPs), including verifying and recording customer identities, screening against terrorist watchlists, and preserving relevant compliance records.

The public comment period will close 60 days after publication in the Federal Register.

CFPB Rescinds 2020 Advisory Opinion on Special Purpose Credit Programs

On June 17, 2026, the Consumer Financial Protection Bureau (CFPB) rescinded its 2020 advisory opinion on Special Purpose Credit Programs (SPCPs) under Regulation B, which implements the Equal Credit Opportunity Act (ECOA). The action effectively withdraws prior interpretive guidance that had clarified how for-profit lenders could structure SPCPs intended to expand credit access to historically underserved groups.

The CFPB explained that the 2020 advisory opinion is now outdated in light of its April 2026 final amendments to Regulation B, which significantly revised how SPCPs are evaluated under the ECOA framework. According to the CFPB, the prior guidance no longer aligns with the current regulatory approach and therefore could create confusion for regulated institutions.

Executive Order Shifts Focus on Immigration Risk in Banking

On May 19, 2026, President Trump issued an executive order, *Restoring Integrity to America's Financial System*, which:

- Directs the Secretary of the Treasury to issue a formal Advisory to financial institutions identifying typologies and "red flags" associated with suspicious activity, including patterns involving payroll tax evasion, use of nominee structures or shell companies, and the use of Individual Taxpayer Identification Numbers (ITINs) in circumstances that may indicate elevated risk.
- Directs the Secretary of the Treasury and Federal financial regulators to consider changes to BSA regulations to strengthen risk-based customer due diligence and customer identification program requirements for covered financial institutions.
- Directs the CFPB to consider clarifying that potential deportation and loss of wages are factors that could adversely affect a non-work authorized borrower's ability to repay an extension of credit under the ability-to-repay standards, and that lenders may consider such factors as part of a reasonable and good-faith underwriting determination.
- Directs Federal financial regulators to issue guidance regarding the management of potential credit risks posed by the non-work authorized population.

USDA FSA-211

We will discuss the United States Department of Agriculture (USDA) Farm Service Agency (FSA)'s Form FSA-211, Power of Attorney, which is used to appoint someone to act on behalf of another as attorney-in-fact.

ABA's Women Lead Symposium

The American Bankers Association's Women Lead Symposium, taking place July 30, 2026, is a virtual event offering banking professionals a convenient opportunity to strengthen leadership skills, gain industry insights, and connect with peers nationwide.

UCC-1 Financing Statement/CNS Reminders

- The UCC-1 Financing Statement and CNS each serve very different purposes. The UCC-1 Financing Statement perfects the bank's security interest and its priority position, while the CNS protects ag buyers when they purchase farm products.
- UCC-1 Financing Statements must provide the "correct debtor name."
    - With an individual debtor, the correct debtor name will generally be the name on the debtor's driver's license.
    - With an entity debtor, the correct debtor name will generally be the name on the documents filed with the secretary of state.
- UCC-1 Financing Statements must be filed with the Secretary of State in the state where the debtor is located.
- You must file the CNS in the state where the agricultural product is sold.

The Executive's AI Playbook

NDBA has made a complimentary resource available through its partnership with the Graduate School of Banking at the University of Wisconsin-Madison (GSB): The Executive's AI Playbook. Developed by expert GSB faculty, this free guide provides clear, actionable steps to help you move beyond the basics and apply AI at your bank.

Upcoming Events

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

- **2026 Regional Member Meetings |** September 14-17, 2026 | Grand Forks, Fargo, Washburn and Minot
- **NDBA Ag Credit Conference |** October 1-2, 2026 | Hilton Garden Inn, Fargo
- **IRA Fundamentals |** October 26, 2026 | Holiday Inn, Bismarck
- **IRA Advanced |** October 27, 2026 | Holiday Inn, Bismarck
- **IRA Fundamentals |** October 28, 2026 | Holiday Inn, Fargo
- **IRA Advanced |** October 29, 2026 | Holiday Inn, Fargo
- **Health Savings Account Seminar** | October 30, 2026 | Holiday Inn of Fargo
- **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

NORTH DAKOTA BANKERS ASSOCIATION

BUSINESS EMAIL COMPROMISE: WHY STRONG WIRE SECURITY PROCEDURES MATTER

Business Email Compromise Remains a Leading Fraud Threat

Business Email Compromise (BEC) continues to be one of the most financially damaging cybercrimes affecting businesses and financial institutions. According to the FBI's 2025 Internet Crime Report, 86% of reported BEC losses involved wire transfers or ACH transactions. Scammers target businesses and individuals who perform legitimate transfer-of-funds request using the following techniques:

Technique	How It Works
Spoof email account or website	Fraudsters create email addresses or websites that resemble legitimate ones (e.g., john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) to deceive recipients.
Send spearphishing emails	Targeted emails trick employees into revealing login credentials or other sensitive information, allowing criminals to access business email accounts, calendars, and payment information.
Use Malware	Malicious software infiltrates company systems, giving criminals access to email threads, invoices, passwords, and financial account information. Attackers often use this information to time fraudulent payment requests so they appear legitimate.
Social engineering and impersonation	After observing legitimate communications, criminals impersonate executives, vendors, or trusted business partners—sometimes using AI-generated voice technology—to convince employees to initiate unauthorized wire transfers.

Source: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

Impact in North Dakota

BEC and wire fraud are not limited to national headlines – they continue to affect businesses across North Dakota. This year, the United States Attorney's Office for the District of North Dakota and FBI seized $4,856,578.51 in money fraudulently obtained from Dickinson Public Schools during a BEC scheme.[1]

UCC Article 4A

Funds transfers, including wire transfers, are governed by Article 4A of the Uniform Commercial Code (adopted in North Dakota as Chapter 41-04.1, N.D.C.C.). Critically, UCC Article 4A determines whether the bank or customer bears the risk of loss for a fraudulent wire transfer. In relevant part, a bank is liable to refund its customer where it "accepts a payment order issued in

[1] https://www.justice.gov/usao-nd/pr/north-dakota-fbi-and-us-attorneys-office-recover-48-million-dollars-scammed-dickinson

the name of its customer as sender which is not authorized and not effective as the order of the customer under section 41-04.1-10..." N.D.C.C. § 41-04.1-12 (4A-204). Stated differently, the bank must refund any wire transfer that is not "authorized" or "effective".

Concept	Description
Authorized	A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency. *N.D.C.C. § 41-04.1-10(1) (4A-202).*
Effective	A payment order is effective as the order of the customer, whether or not authorized, if: • The bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified under a security procedure; and • The security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and • The bank proves that it accepted the payment order in good faith and in compliance with the bank's obligations under the security procedure and any agreement or instruction of the customer, evidenced by a record, restricting acceptance of payment orders issued in the name of the customer. *See N.D.C.C. § 41-04.1-10(2) (4A-202).*

BEC-related wire fraud may involve scenarios in which a payment order is authorized (i.e., the authorized party was manipulated by a scammer but issued the payment order) or unauthorized (i.e., unauthorized party impersonated customer).[2] However, as noted above, even if a payment order is not authorized by the customer, it may be "effective" if the listed requirements are met. As a result, the risk of loss for an unauthorized wire transfer may shift away from the bank through the proper use of security procedures.

Security Procedure

"Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of verifying that a payment order or communication amending or canceling a payment order is that of the customer or detecting error in the transmission or the content of the payment order or communication. *N.D.C.C. § 41-04.1-09 (4A-201).* A security procedure may impose an obligation on the receiving bank or the customer and may require the use of algorithms or other codes, identifying words, numbers, symbols, sounds, biometrics, encryption, callback procedures, or similar security devices. *Id.* Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer or requiring a payment order to be sent from a known electronic mail address, internet protocol address, or telephone number is not by itself a security procedure. *Id.*

[2] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

Commercial Reasonableness

Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. *N.D.C.C. § 41-04.1-10(3) (4A-202)*. A security procedure is deemed to be commercially reasonable if the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and the customer expressly agreed in a record to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the bank's obligations under the security procedure chosen by the customer. *Id.*

Key Takeaways

As BEC schemes continue to evolve, financial institutions should regularly review their wire transfer security procedures, document customers' acceptance of available security options, and educate commercial customers about the risks of email compromise. Layered authentication, independent verification of payment requests, and periodic review of wire transfer controls remain among the most effective tools for mitigating fraud and strengthening a bank's position under Article 4A.

TRUSTED CONTACTS

A "trusted contact" is an individual that a bank may contact if they suspect that the accountholder is a victim or target of financial exploitation. Trusted contacts are authorized and governed by Section 6-08.5-04 of the North Dakota Century Code, which provides as follows:

6-08.5-04. Individuals who may be contacted regarding suspected financial exploitation - Immunity - Exemption from customer consent and notice provisions.

1. A financial service provider may offer to an eligible adult the opportunity to submit and update periodically a list of individuals the eligible adult authorizes the financial service provider to contact if the financial service provider has reasonable cause to suspect the eligible adult is a victim or a target of financial exploitation.
2. Notwithstanding subsection 1, a financial service provider having a good faith belief to suspect an eligible adult is the victim or target of financial exploitation may convey the suspicion to one or more of the following individuals, provided the individual is not the suspected perpetrator:
   a. An individual on the list described in subsection 1.
   b. A co-owner, additional authorized signatory, or beneficiary on the eligible adult's account.
   c. An attorney-in-fact, trustee, conservator, guardian, or other fiduciary who has been selected or appointed to manage some or all of the financial affairs of the eligible adult.
3. If a financial service provider provides information under this section, the financial service provider may limit the information, such as disclosing only that the financial service provider has reasonable cause to suspect the eligible adult may be a victim or target of financial exploitation, without disclosing any other details or confidential personal information regarding the financial affairs of the eligible adult.
4. The financial service provider may choose not to contact an individual on the list provided under subsection 1, if the financial service provider suspects the individual is engaged in financial exploitation.
5. The financial service provider may rely on information provided by the eligible adult in compiling a list of contact individuals.
6. A financial service provider, or an employee, officer, or director of a financial service provider, is immune from all criminal, civil, and administrative liability for contacting an individual or electing not to contact an individual under this section and for actions taken in furtherance of that determination if the determination is made based on a good faith belief financial exploitation occurred, was attempted, or is being attempted.
7. Contact with an individual, and any information provided under this section, is exempt from the customer consent provisions in sections 6-08.1-03 and 6-08.1-04.

To assist financial institutions in implementing trusted contact programs, the CFPB has developed a Trusted Contact Guide. In addition, a sample trusted contact form is provided on the next page. Banks should review any trusted contact program, forms, and procedures with counsel.

NORTH DAKOTA BANKERS ASSOCIATION

TRUSTED CONTACT LIST

__________________ (“account holder”) hereby designates the following people to be “Trusted Contacts”:

Trusted Contact 1

Name: _______________________________ Phone Number: __________________________

Address: ____

Email Address: ____

Relation to Account Holder: ____

Trusted Contact 2

Name: _______________________________ Phone Number: __________________________

Address: ____

Email Address: ____

Relation to Account Holder: ____

Account holder’s Trusted Contacts will be contacted by the bank if the bank has concerns or suspicions the account holder is a victim of financial exploitation or is experiencing a decline in mental capacity. Signing this Trusted Contact List does not authorize Trusted Contacts any power over the account. Trusted Contacts are simply contact references in the case of suspected exploitation.

Signed this ____ day of July, 2026.