



2026 Annual Compliance and Security Bulletin

Thank you for choosing us as your financial partner. Together, we'll navigate the ever evolving compliance and security landscape and empower your *incredible*.

In this issue:

- **Page 1** - Learn what you need to do now to comply with the 2026 Nacha Rules changes.
- **Page 2** - Dive deeper into the Nacha Rules and learn how to obtain a copy of the Nacha Rules Book.
- **Page 3** - Review all the requirements of a Nacha-compliant Consumer Debit Authorization (Free sample included!)
- **Page 4** - We reveal what you can do to safeguard your business from cyber attacks.
- **Page 5** - We've got you covered! Links to additional resources we think you'll love.

IMPORTANT UPDATE: 2026 ACH RULES CHANGES

EFFECTIVE NOW

Standardized Company Entry Description for Payroll Entries

To improve fraud monitoring efforts and transparency across the ACH Network, Nacha now requires the use of the word **PAYROLL** (all caps, no space) as the Company Entry Description for all PPD credit entries for wages, salaries, and other similar types of employee compensation. Please review your ACH templates used for payroll entries and confirm the Company Entry Description is exactly PAYROLL. Other descriptions such as SALARY, PAY, PAYMENT, DIRECT DEPOSIT should be replaced with the word PAYROLL.

EFFECTIVE JUNE 22, 2026

New Fraud Monitoring Requirement for ACH Originators

Starting on June 22, 2026, all businesses that originate ACH transactions will be **required to implement and document risk-based fraud monitoring processes and procedures**. This includes processes designed to identify ACH entries that may be unauthorized or fraudulent.

WHAT DOES “RISK-BASED” MEAN?

Nacha does not mandate a one-size-fits-all solution. Instead, your fraud monitoring should be appropriate for the size, complexity, and risk profile of your ACH activity. Here are some best practices you might consider:

- Ensure all your company's online users have their own set of carefully safeguarded login credentials.
- Train all employees to never share their password or 2FA code with anyone.
- Implement dual control for ACH Origination (Ask us how!)
- Ensure all debit entries are properly authorized by the receiver before initiation.
- Verify all invoices and direct deposit authorizations are legitimate before initiating payment.
- Utilize ACH prenotes or third-party account validation services to confirm validity and ownership of a new vendor or employee account before live payment is sent.
- **This one's important!** Ensure all vendor & employee account change requests are properly verified before payment is redirected to a new account.
 - **In-person requests** for account changes should include photo ID verification.
 - **Phone and email requests** should include a callback to a known, previously collected phone number. Caller ID and email “from” fields should not be relied upon as they are easily spoofed by fraudsters.

NACHA RULES OVERVIEW

The Nacha Operating Rules are the foundation for every ACH payment. By defining the roles and responsibilities of financial institutions and establishing clear guidelines for each Network participant, the Rules ensure that millions of payments occur smoothly and easily each day.

A few highlights of the Nacha Operating Rules:

- If you receive a Notification of Change (NOC) indicating a correction is needed on an entry previously sent, you must make the correction within six (6) banking days or prior to initiating another entry to the Receiver's account.
- If an ACH entry is returned to you because of Closed Account or No Account Found at the Receiver's Financial Institution, you must correct the account information within six (6) banking days or prior to initiating another entry to the Receiver's account.
- If an ACH entry is returned to you Unauthorized, you must obtain a new authorization from the Receiver within six (6) banking days or prior to initiating another entry into the Receiver's account.
- If an ACH entry is returned to you because of Insufficient Funds, you may only resubmit two (2) more times in an attempt to clear it. Both entries must be made within 180 days of the settlement date of the original entry and contain **RETRY PYMT** (all caps, with space) in the Company Entry Description field.
- If an outgoing ACH entry is transmitted to a consumer account, it must be coded as a PPD. If transmitted to a non-consumer account, it must be coded as a CCD.



CONSUMER DEBIT AUTHORIZATION REQUIREMENTS

Prior to initiating a debit entry to a consumer account, the business initiating the entry must obtain proper authorization. Authorization must be in writing or similarly authenticated, must be clearly identifiable as an authorization and understandable to the consumer and must contain the following:

- Date of authorization
- Consumer (Receiver) name
- Consumer account information (routing and account number + account type)
- Originator (merchant/company) name
- Clear authorization statement permitting ACH debits
- Timing of debits (one-time, recurring, or standing authorization)
- Amount or method for determining the amount
- Instructions on how to revoke the authorization
- Consumer's signature or similar authentication

Here's a sample of a Nacha-compliant debit authorization. To request an editable version, please email cashmanagement@incrediblebank.com.

[YOUR COMPANY LOGO]
DEBIT AUTHORIZATION FORM

I (we) hereby authorize **[YOUR COMPANY NAME]**, hereinafter called "COMPANY", to initiate electronic debit entries to my (our) account indicated below and IncredibleBank, hereinafter called "FINANCIAL INSTITUTION", to debit the same to such account for the purpose of **[PURPOSE OF DEBIT]**. I (we) acknowledge that ACH transactions I (we) authorize must comply with all applicable laws, including U.S. law. In the event of an erroneous or duplicate entry, I hereby authorize **[YOUR COMPANY NAME]** to credit my account indicated below to correct any error made.

Accountholder Name: _____ Checking Savings
Routing Number: _____ Account Number: _____
Amount of debit or method of determining amount: _____
Frequency of debit: (one-time, weekly, monthly, etc.): _____
Date of debit (If recurring, indicate start date): _____

This authorization will remain in full force and effect until COMPANY has received written notification from me (or either of us) of its termination in such time and manner as to afford COMPANY a reasonable opportunity to act on it.

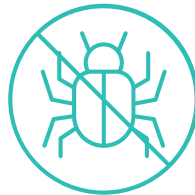
Print Name: _____
Signature: _____ Date: _____

PROTECT YOUR BUSINESS FROM A CYBER ATTACK!



Spam email

Most attacks will originate in your email. Secure your email using SPAM filters and other tools.



Anti-virus

Make sure you leverage anti-virus and anti-spyware tools on all your devices. New viruses come out every day so it is important that these are kept up-to-date.



Passwords

Enforce password security. The longer the better. Use passphrases instead of common words. Never share passwords and avoid using the same password for all your applications and accounts. Enable multi-factor authentication (MFA).



Mobile devices

Mobile devices are computers. Today's criminals attempt to steal data or access your network through your (and your employee's) mobile devices. Enforce passwords, biometrics and other mobile device security functionality.



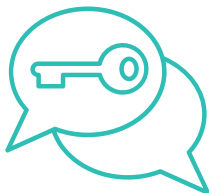
Computer updates

Keep your network and applications such as Microsoft, Adobe and Java up to date.



Backup

Backup local. Backup to the cloud. Have an offline backup and test your backups often.



Security awareness

Train your users...often. Teach them about data security, email attacks, and your security policies and procedures.



Cyber insurance

When all else fails, protect your income and business with cyber insurance policies.



Two-Factor Authentication

Instead of phone/text codes, use high-security 2FA methods, such as Security Keys or passkeys.

LINKS AND RESOURCES

To obtain a free copy of the Rules:

1. Go to www.nachaoperatingrulesonline.org.
2. Click **Claim Your Subscription**.
3. Type in your email address and click **Continue**.
4. Check the box for **No Subscription Code** and enter your personal information.
5. Check the box to agree to the Terms of Use.
6. Click **Redeem**.
7. Click the blue button to **Log In**.
8. Enter your email and temporary password (provided to you in an email from digital@omnipress.com).
9. Click **Login**.
10. Select **Resources** to access a free (basic) copy of the Rules or purchase a more interactive version from this site.

Plan ahead with confidence!

Visit www.incrediblebank.com/holiday-calendar for a complete list of all the upcoming holidays that impact our branch hours and payment processing schedules.



Cybersecurity Tips and Tricks for Business Owners

Stay vigilant, stay curious and stay secure. Check out the Cybersecurity page on our website for more tips and tricks.

IncredibleBank Blog

Discover the latest fraud tactics and dodge them like a pro. Our blog features articles designed to help you block fraudsters from accessing your information and your money.



Get in touch with us!

1-888-842-0221

info@incrediblebank.com

You can even send us a message right in the IncredibleBank mobile app or online banking.

Look for "Messages" to get started!