Is this email not displaying correctly?
View it in your browser.

PAYMENTS BULLETIN

In This Issue

Altera Payroll & Insurance First Edition Newsletter Is Here!

Altera Payroll & Insurance's (API) is dedicated to ensuring our clients receive the most updated information on payroll solutions that impact your business. As provided in our ACH Agreement, all participants within the ACH network must comply with *NACHA Operating Rules*. We want to take a few moments to break down the meaning of complying with *NACHA Operating Rules.*

What Does This All Mean?

When you sign your ACH agreement with us, you agree to comply with *NACHA Operating Rules* and all U.S. laws. This means that you must follow *NACHA Operating Rules* and comply with U.S. law when sending and/or receiving ACH entries. NACHA is the network rules governing body when we use the ACH network for processing.

Tips for Complying with NACHA Operating Rules

- Understand your requirements to comply with the *NACHA Operating Rules* and ask us to explain something that you may not understand;
- When receiving exception items such as returns and/or notifications of change, act on them immediately. Remember, exception item handling is time sensitive. You are

required to resolve an exception with your Receiver or terminate the authorization and not resubmit;
- If you change your security procedures and/or have significant changes to your process, let us know – we are here to ensure you are compliant and want to provide you with as much support to make changes with the appropriate risk management controls.

A Reminder About Your Responsibilities When Receiving Unauthorized/Revoked Consumer Debit Entries

ACH Originators should expect the possibility that a Receiver of a debit may return the entry as unauthorized or revoked. As an API value added service, you receive your returns and notifications of change via a secured network directly from the Federal Reserve Bank to allow faster turnaround on handling your exception items. An unauthorized debit entry is an entry in which:

- The authorization requirements have not been followed in accordance with the Rules or invalid under applicable legal requirements.
- A transaction was initiated in an amount different than that authorized by the Receiver.
- A transaction was initiated for settlement earlier than authorized by Receiver.

A revoked entry is used when the Receiver has provided notice that the authorization for the debit entry was revoked directly with the Originator under the terms and conditions set forth in the authorization agreement.

When you receive an unauthorized or revoked entry, it is your responsibility to obtain a new authorization from the Receiver or cancel the transaction. The absence of this procedure of the Originator could result in a network violation.

Educate & Protect Yourself from Cyber Fraud

The National ACH Association (NACHA) has recently posted information on a suspicious email that appears to come from the National ACH Association. As a payroll client, it is important to know when an email is suspicious, as fraudsters target businesses of all sizes every day. NACHA has also posted important information relating to these types of emails to better protect your organization.

- NACHA does not process nor otherwise touch the ACH transactions that flow via the ACH network nor between financial institutions and their customers.
- NACHA does not send communications of any type to persons or organizations about individual ACH transactions that they originate or receive.
- NACHA is the industry trade association that manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data.
- The ACH Network serves as a safe, secure, reliable network for direct consumer, business and government payments, and annually facilitates billions of payments

such as Direct Deposit or Direct Debit.
- These incidents are occurring with greater frequency and increased sophistication. Perpetrators are conducting similar phishing attacks in which they are sending fraudulent emails that claim to be from the Federal Reserve Bank, IRS, other federal agencies, as well as commercial financial institutions, other payment organizations, technology companies and businesses[1].

---

[1] www.nacha.org/news/fraudulent-emails-appearing-come-nacha-educate-yourself

Fraud Prevention Corner

Here are some tips to stay safe online and help protect your money:

- **Use multiple passwords.** Don't use the same password for your online banking that you use for anything else. And remember not to use easily guessed passwords — use symbols and numbers to make your password harder to guess or engineer. Many fraudsters use software to test thousands of passwords to hack accounts, and complicated ones are harder to crack.
- **Enable two-step verification.** Gmail, Facebook, Twitter and Apple iCloud all offer a double layer of protection on your accounts, so logins from unknown devices require a second password that is texted to you. This extra layer of security prevents others from accessing your personal information without access to your phone.
- **Limit the amount of personal information you post.** Be especially guarded with your address or information about your schedule or routine. And make sure you monitor what your connections post about you.
- **Evaluate your settings.** Sites like Facebook change their privacy options, so review your security and privacy settings regularly. To be safe, in case settings change unexpectedly, don't post anything that you wouldn't want the public to see.
- **Be wary of third-party applications.** Use caution when deciding which applications to enable and, when possible, limit the amount of information the applications can access. Think about third party applications that connect using your Facebook or Twitter account for an easier registration and login — make sure you only enable ones with companies you know and trust.
- **Be on the lookout for imposter fraud in social media.** Be very cautious about connecting with people you don't know or recognize. Fraudsters create fake personas and try to connect with multiple people from one organization — like your high school or college — so they look like a mutual acquaintance. Then, once you're connected, this person sends malicious links through email, chat, videos or a direct message. If you click it, your device will likely be compromised and that imposter now has access to more easily hack into your accounts and files.

For all this information and more, visit
alterapayroll.com or call us at **478.477.6060**

Are Not a Deposit	Are Not FDIC-Insured	May Go Down In Value
Are Not Guaranteed by the Bank	Are Not A Condition to Any Banking Service or Activity	Are Not Insured by Any Federal Government Agency

Altera Payroll & Insurance | alterapayroll.com
201 Sheraton Blvd., Macon, Georgia 31210

Copyright © 2017, All rights reserved.

Our mailing address is:

State Bank and Trust Company
3399 Peachtree Road, Suite 1830
Atlanta, GA 30326

unsubscribe from all emails | update subscription preferences