MIDSTATES BANK

BUSINESS BANKING

Cash Management

(888) 710-9070
www.MidstatesBank.com
CashManagement@msbna.com

MIDSTATES
BANK

RE: Digital Banking Upgrade/ACH Origination Education

We are excited to announce that we will be upgrading our **Digital Banking and Cash Management platform** to provide you with an enhanced banking experience featuring improved functionality, security, and convenience. **September 21, 2026** is the official **Go Live date** for our new digital banking platform. You will continue to access online banking through our website just as you do today.

To help you prepare for the transition, we have enclosed a **Digital Banking Conversion Guide and Cash Management Brochure** that answers common questions and outlines any steps you may need to take before the conversion. We encourage you to review these documents carefully and retain it for future reference.

Also included is the **ACH Rules and Updates for Business Originators – 2026 Newsletter**, which contains updated debit, credit, and recurring debit authorization forms; **ACH User Quick Reference Card**, a valuable resource for corporate ACH originators. This guide provides quick access to important ACH processing information, including:

- ACH returns and dishonored returns
- Standard Entry Class (SEC) codes
- Transaction codes
- Notifications of Change (NOCs)

Additionally, you will find the **Fraud Advisory for Businesses: Corporate Account Takeover**, which outlines current cyber threats and recommended best practices to help protect your organization from fraud and cybercrime.

We encourage you to review all enclosed materials to familiarize yourself with the upcoming digital banking enhancements and important ACH updates.

If you have any questions, please do not hesitate to contact a member of the Cash Management Support Team.

Thank you for your continued business and trust in Midstates Bank.

Cash Management Support Team
CashManagement@msbna.com
888-710-9070

CONTACT **US**

Website
www.midstatesbank.com

Phone
888-710-9070

Email
cashmanagement@msbna.com

DIGITAL BANKING UPGRADE

We're excited to provide you with an enhanced banking experience featuring improved functionality, security, and convenience.

When Do the New Services Go Live?
September 21, 2026 is the official Go Live date for our new digital banking platform.
You will continue to access online banking through our website just as you do today.

Will I Use the Same Login Credentials?
Yes. Your existing Username will carry over to the new digital banking platform.
During your first login, you will complete a one-time setup process:

- Your current Username will remain the same.
- Your temporary password will be the last four digits of your company's Tax Identification Number (TIN).
- You will be prompted to create a new password during the initial login process.

CASH MANAGEMENT

Where will I find Cash Management Services?

All services previously found under the Cash Management tab will move to the new digital banking platform and will continue to be labeled Cash Management for easy access.

Will user access remain the same?

Yes. Existing users and permissions will convert to the new platform. We recommend that company administrators review user access after conversion and make any necessary updates.

Will my existing ACH batches convert?

Yes. All ACH batches will transfer to the new system, and 90 days of ACH batch history will be available. Please save any older history you may need before September 19, 2026.

What services are available in Cash Management?

- ACH Origination
- Remote Deposit Capture (RDC)
- Wires
- Positive Pay
- Other business banking services you use today

ACH ORIGINATION

ACH Origination gives businesses an easy, reliable way to move funds electronically for common needs like payroll and accounts payable.

Our platform lets you upload ACH files or key them in manually, edit and resubmit as needed, and ***set up recurring ACH payments*** for added convenience and efficiency.

REMOTE DEPOSIT CAPTURE

Make depositing checks faster, easier, and more efficient—right from your workplace.

- Use a secure, in-office scanner to quickly process incoming checks whenever it fits your schedule and transmit images through your office network
- Improve cash flow with faster access to deposited funds
- Generate clear, detailed summaries of each day's deposits
- Search archived check images or view all payments from a specific customer

WIRES

Midstates Bank's Online Wire platform gives you a fast, convenient way to initiate wire transfers. Create and save templates for recurring wires, so you don't have to re-enter payment details each time.

POSITIVE PAY

Positive Pay is a fraud-prevention service that allows you to review the details of checks written against your account to make sure transactions are legitimate.
Now, accessible from your mobile device!

- Remain in control over your account's activity
- Daily review and indicate whether charges should be paid or returned
- View online for transaction exception approval or denial.

OTHER SERVICES

- Notary Services
- Credit Cards
- Cashier's Checks
- eStatements

MIDSTATES BANK

Digital Banking + Cash Management Conversion Guide

This guide is provided as a convenience to help you prepare for the transition to our new **Digital Banking and Cash Management** platform, live **Monday, September 21, 2026**.

Before Conversion

- ☐ **Review the Cash Management Resource & FAQ page** [↗]
  - Understand how your data will appear in the new platform.
- ☐ **Confirm active users and verify contact details.**
  - Phone number, SMS-enabled mobile number, and email address.
  - Your banker will also review user alerts and security and controls.
- ☐ **Mark your calendar for important dates.**
  - **Friday, September 18 (4:00 PM) through the morning of Monday, September 21**: Online and Mobile Banking will be in view-only mode while we migrate the system.
  - **Monday, September 21**: The new Digital Banking and Cash Management platform goes live.

Week Before Conversion

- ☐ **Review upcoming ACH payments**.
  - To avoid delays during the conversion, process payments that would normally be scheduled for Monday or Tuesday by **4:00 PM on Friday, September 18**.
- ☐ **Complete Accounting Software File Backups**
  - Download a data file backup and final transaction download by **2:00 PM on Friday, September 18**. Review the Accounting Software **Conversion Guide** before you begin. [↗]
- ☐ **Save ACH Batch History** (*Optional*)
  - Only 90 days of ACH batch history will migrate. Save older history and any master batches you want to retain by **September 18**.
- ☐ **Review the First-Time Login Instructions** [↗] to prepare for initial sign-in.

Conversion Week

- ☐ Confirm you can log in as expected once the new platform is live.
- ☐ Review scheduled and recurring payments for accuracy.
- ☐ **Confirm access to applications through the Cash Management tab**.
  - ACH, Positive Pay, Wire, Remote Deposit Capture, and Settings/Permissions.
- ☐ **If you originate ACH or wire transactions, complete Duo Soft Token enrollment.**
  - Your banker will assist with this process.
- ☐ **Reconnect your accounting software.**
  - Deactivate and reactivate the connection, then confirm no transactions were duplicated or missed on your register.

Questions or need assistance?
Contact your Business Banker • CashManagement@msbna.com • 888-710-9070

MIDSTATES BANK

Important Dates

Date	What Happens
September 18, 4:00 PM	Online and Mobile Banking move to view-only mode through the morning of Monday, September 21, while we migrate the system. You'll still be able to view balances and transactions, but ACH, wires, transfers, bill pay, and remote deposit will be unavailable. [↗] **Accounting software:** Complete a data file backup and a final transaction download today. See Accounting Software Conversion Guide. [↗]
September 21	The new Online and Mobile Banking platform is live. If you use the Midstates Bank Mobile Banking App, you'll be prompted to update to the newest version.
On or after September 22	For accounting software: complete the remaining conversion steps, including deactivating and reactivating your online banking connection.

Frequently Asked Questions

General Conversion & Timeline

1. When do the new services go live?

Monday, September 21, 2026, is the go-live date for our new digital banking solutions.

2. What is the web address for Midstates Bank's new online banking site?

You'll still log in from MidstatesBank.com, just as you have in the past. Please bookmark the new website address. Users will be prompted to authenticate with a six-digit code sent by text, email, or automated phone call at login. ACH and wire originators will also be offered Duo soft tokens for those services.

Login, Security & Access

3. Will I be able to log in with the same credentials I used before conversion?

Yes. The new Digital Banking platform will require a one-time setup. Your username will carry over to the new platform, and your temporary password will be **the last 4 digits of your company's TIN**. You'll be prompted to change it during your first login.

4. Will I have access to my accounts and Cash Management through the mobile app?

Yes. The new digital banking platform gives you a seamless experience across desktop and mobile. Follow the prompt to download the new app from the Google Play Store or Apple App Store.

New App Icon

5. Why do I need an identity verification code?

We've added an Out of Band Authentication step to protect your accounts in place of tokens at login. You'll be asked to enter a 6-digit security code, which you can receive by text, email, or automated phone. If your preferred method isn't listed, contact the bank to update your contact information. To skip this step on future logins, you can mark your computer or device as trusted. You may store up to 5 trusted devices (computer, phone, tablet, etc.)

6. Will users be required to have tokens for business payment services?

We've replaced tokens with an Out of Band Authentication step at login. If you originate ACH or wire transfers, we'll need your phone number on file for enhanced authentication using soft tokens. Your banker will assist with setting up this process during the week of conversion. If you're not sure whether we have your current cell number, please call Midstates Bank to update your contact information.

7. Will business user access remain the same?

Yes. User information and access levels will be converted, but some details may appear differently in the new platform. We recommend that your company's administrator review user access during conversion and make any necessary updates.

8. Can I customize my account list?

Yes. In the new digital banking platform select your User Profile, then click and drag accounts in the Order column to arrange them in your preferred viewing order. To hide an account, select Hide on the right.

Transfers, Payments & Bill Pay

9. What will happen to internal future-dated and recurring transfers (between Midstates Bank accounts) that I previously set up?

Previously scheduled internal future-dated and recurring transfers, including loan payments, will be converted to the new digital banking platform. Once you're logged in, you can view, modify, or delete any transfer that was previously created.

10. Will my Bill Pay stay the same?

Yes. If you're a current Bill Pay user, your payment history, payees, and scheduled payments will carry over. You'll likely need to accept an updated disclosure the first time you access Bill Pay. From there, you'll use the Bill Pay menu just as you have in the past.

Cash Management & Business Services

11. How will I access services previously listed under the "Cash Management" tab?

All Cash Management features will move to the new platform under Cash Manager. For assistance, contact Cash Management Services at 888-710-9070, email CashManagement@msbna.com, or send a secure message in the app or online.

12. What business services will be listed under the "Cash Management" tab?

ACH, Wires, Positive Pay, Remote Deposit Capture and Payee Directory, along with the other services you already expect from our Digital Banking solutions

13. I don't have a "Cash Manager" tab, but I'm interested in these services. How do I enroll?

Contact Business Services by calling 888-710-9070 or sending us a secure message.

14. Will my Cash Management alerts stay the same?

Yes. Alerts you've already set up will be transferred to the new digital banking platform. Your banker can also help you set up new alerts for ACH, ACH Same-Day, and Wire initiation.

15. How do I access Remote Deposit Capture?

Access Remote Deposit Capture through a drop down in Cash Manager. If you're not a Cash Management customer, you'll still log in from midstatesbank.com and select Remote Deposit, just as you have in the past.

ACH Origination

16. Will my existing ACH origination batches convert?

Yes, all ACH batches will convert, and 90 days of ACH batch history will be available after conversion. Please save any batch history older than 90 days, as well as any master batches you'd like to retain before conversion on September 18, 2026.

17. Will there be any difference in the ACH origination process?

The Dual Control process will remain the same after conversion:

- **Approval Pending:** The ACH batch is new or has been processed before and is ready to be processed again. If it was previously created, a user must click "Approve" to move it to the next status.
- **Uploaded:** A batch uploaded through Import Batch, ready to be approved. It must be approved before it can be edited or initiated.
- **Ready to Initiate:** The batch has been approved and is ready for a second user to initiate. To meet dual control requirements, this step can't be done by the same user who approved the batch. (If your company doesn't use Dual Control, this and the approval step can both be completed by the same user.)
- **Initiated:** The batch has been initiated and is considered complete. The Send and Effective Dates will display in their respective columns, and the batch will show as Ready once it has processed.

18. Can I set up recurring ACH payments?

Yes. You can arrange recurring ACH debits and credits directly through the new platform under ACH, with scheduled payments up to one year in advance.

Accounting Software Integration (Quicken / QuickBooks)

19. Will I still be able to use Quicken and/or QuickBooks WebConnect or Express WebConnect with the new online banking? Will I need to reconnect my accounts, and how do I sync my software to the new platform?

Yes. WebConnect and Express WebConnect will be available with the platform for use with Intuit's Quicken and QuickBooks products. This update will require action on your end to ensure a smooth transition:

- **1st Action Date (On or before September 18, 2026, by 2:00 PM):** Complete a data file backup and a final transaction download. Transactions may not be available for download after this date. (See Accounting Software Conversion Guide for step-by-step instructions.) [↗]
- **2nd Action Date (On or after September 22, 2026):** Complete the remaining conversion steps, including deactivating and reactivating your online banking connection. This ensures your Quicken or QuickBooks accounts are correctly connected to our new platform.

Note: *If you use Express WebConnect or an online version of Quicken or QuickBooks, it will take Intuit 2 to 5 business days from September 22 to point your connection to Midstates Bank's new system.* ***During that window, the aggregated connection will be down****. As an alternative, you can manually download account activity into Quicken or QuickBooks using WebConnect (select Transactions > Export). Please review your downloaded transactions carefully after migration to prevent duplicates or missed entries.*

MIDSTATES BANK

Information Migration Guide

Digital Banking Platform Conversion + Cash Management Users

Type of Information	Migration Information	Action
Online Banking	One-time setup required. Your username will remain the same. Your temporary password will be the last four digits of your company's TIN and must be changed first login.	**Action Required**
Mobile App	Update to the latest app version. Cash Management features will be available in the mobile app.	**Action Required**
Accounting Software	**By September 18, 2026, at 2:00 PM:** Complete a backup and final transaction download. **On or after September 22, 2026:** Deactivate and reconnect your online banking connection.	**Action Required**
Security Token	Login tokens are now replaced by Out of Band Authentication. ACH and wire originators: your banker will assist with setting up soft-token phone authentication during conversion week	**Action Required**
Users & User Roles	Users and roles will migrate. Please verify email addresses and SMS-enabled mobile numbers for all users.	**Optional Action**
ACH Batches	Only the most recent 90 days of ACH batch history will migrate. Save older history and any master batches by **September 18, 2026**.	**Optional Action**
Alerts	Existing alerts will migrate automatically. Contact your banker to set up new alerts for ACH, Same-Day ACH, or wires.	**Optional Action**
Accounts	Active accounts, access permissions, and account nicknames will migrate.	**No Action Required**
Bill Pay	Bill Pay payees will migrate.	**No Action Required**
Internal Transfers & Loan Payments	Scheduled and recurring internal transfers, including loan payments, will migrate.	**No Action Required**
eStatement Preferences	eStatement preferences will migrate.	**No Action Required**
Stop Payment Requests	Existing stop payment requests will continue to process normally but will not be visible after conversion. Retain your own records if needed.	**No Action Required**
Secure Message History	Secure message history will not migrate. Save any messages you wish to keep before conversion.	**Not Migrated**

MIDSTATES BANK

2026 Originator Newsletter

January 2026

Nacha's role in ACH

Nacha®, the National Automated Clearing House Association, is a trade association that helps develop, implement and enforce rules governing the use of the Automated Clearing House network. Nacha creates rules and standards through consensus-led governance with collaboration and input from industry stakeholders. You can learn more about Nacha by visiting **their website**.

As an ACH Originator, understanding the ACH Operating Rules is essential in ensuring your compliance with the rules. If you wish to purchase a copy of the Rules, you may purchase it at the **Nacha store**, or by contacting your ODFI to receive a copy at your expense.

Upcoming Rule changes

New Company Entry Description Rules take effect March 20, 2026

Company Entry Description – PAYROLL

The Company Entry Description field must contain PAYROLL, all capitalized, for PPD Credits paying wages, salaries and other similar types of compensation. New language indicates that the use of the term PAYROLL in this field is descriptive. By use of the word, neither the Originator, nor the ODFI or any third-party service provider acting on behalf of an Originator or ODFI, makes any representation or warranty to the RDFI or the Receiver regarding the Receiver's employment status.

Company Entry Description – PURCHASE

The Company Entry Description field must contain PURCHASE, all capitalized, for e-commerce purchases. For this purpose, an e-commerce purchase is a debit entry authorized by a consumer receiver for the online purchase of goods, including recurring purchases first authorized online. An e-commerce purchase uses the WEB debit SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL debit SEC Code.

Originators are encouraged to begin using the new PAYROLL and PURCHASE descriptions as soon as possible, but no later than **March 20, 2026**. For more details on the new Company Entry Description requirements, visit **Nacha's website**.

New fraud monitoring requirements take effect March 20 and June 19, 2026

Starting in 2026, business Originators will be required to establish and implement risk-based fraud monitoring processes and procedures reasonably intended to identify ACH Entries initiated due to fraud. The Originator's processes and procedures must be designed to reasonably identify entries suspected of being unauthorized or made under false pretenses, and they must be reviewed and updated at least annually to address evolving risks. These rule changes are part of Nacha's new risk management rules and fraud prevention requirements.

The new fraud monitoring requirements go into effect **March 20, 2026**, for businesses with ACH origination volume greater than six million entries in 2023 and **June 19, 2026**, for businesses that originate less than six million entries annually.

A common question we hear is: What practical steps should Originators, large or small, take to comply?

To keep it simple, most ACH transactions are sent to the same Receivers whether payroll, utility payments, vendor invoices or accounts payable. So, it makes sense to focus on transactions that are unusual or non-recurring. Originators should consider focusing their processes and procedures on brand-new Receivers and existing Receivers who suddenly change account information.

New Receivers

A new relationship needs to be established before sending an ACH credit. First, Originators should perform best practice due diligence reviews to ensure the individual or business is legitimate through verifying identification, performing background checks and ensuring that the proper signers and authorized personnel represent a real entity. Then, Originators should securely store the account information in an encrypted fashion and maintain a valid contact number on file for any future verification.

Existing Receivers who suddenly change account information

If a long-time Receiver unexpectedly sends new account details, especially via email, text or fax, treat it as a red flag. The Originator should use the contact information on file, not the information in the change request message, to verify account changes. Apply "know your customer" practices to confirm the request is legitimate before proceeding. Your company is responsible for following up on any request to change a Receiver's account information with a phone call to the number on file in your records, without relying on the contact information included in the request.

For more details regarding the new fraud monitoring requirements, visit **Nacha's website**. Chapter 15 in the 2026 Nacha Rule book, specifically pages OG74-OG80, provides additional guidance to help Originators implement the new requirements. You can also read **Nacha's blog** for additional tips that'll help Originators comply with the upcoming risk management rules.

Compliance with existing Nacha Rules helps Originators mitigate fraud risk

Secure transmission of ACH information

According to section 1.7 of the ACH Rules, sensitive account information such as the routing transit numbers, account numbers or the entries themselves, must be securely transmitted via encryption or a secure session. Thus, any Originator who's transmitting account information via clear-text or unencrypted email is in violation of this Rule and is being exposed to fraud. Since Originators have direct relationships with Receivers, they're in the best positioned to spot red flags, like new account setups or unexpected changes, and should have escalation processes in place to investigate before transmitting any unusual or suspicious entries.

Originator must obtain authorization from the receiver

Section 2.3 of the Nacha requires Originators to obtain authorization from the Receiver to originate one or more entries to the Receiver's account. This authorization must comply with applicable legal requirements, meaning it must clearly link the Receiver to the consent provided. Common, easily spoofed methods like email don't meet this standard. Instead, secure and traceable authorization methods, such as HR portals, written authorizations, or voided checks, could be used to protect both parties and ensure compliance.

ACH data security

Nacha Operating Rules require all ACH participants to protect the security and integrity of certain ACH data throughout its lifecycle. Your company plays a vital role in maintaining proper security over protected information obtained as an ACH payment Originator. In the context of payment originations, protected information may be referred to as non-public personal which includes the financial information of a natural person used to create an entry, or contained within an entry, and any related addenda record. Originators must be vigilant in their effort to protect the security of protected information due to the increased focus on privacy of data, threats from data breaches and other unscrupulous activity, such as corporate account takeovers, viruses, network intrusions, employee/email fraud and hacking.

Your company is required to establish, implement and update policies, procedures and systems including controls with respect to the initiation, processing and storage of protected information that are designed to:

- Protect the confidentiality and integrity of the protected information until its destruction.
- Protect against anticipated threats or hazards to the security or integrity of protected information until its destruction.
- Protect against unauthorized use of protected information that could result in substantial harm to a natural person.

Chapter four of the 2026 Nacha Rule book, pages OG24-OG28, provides guidance to help Originators comply with the ACH Data Security rules, which also helps mitigate fraud risk.

2026 standard Federal Reserve Bank holidays

The FedACH holiday schedule is published and available on the Federal Reserve **website**. Keep in mind that a payment can't have an effective date on a federal holiday because the Federal Reserve isn't open for processing. Therefore, it's important that you take note of the holiday schedule to make sure the transactions you initiate process on time.

2026 holidays

New Year's Day
Thursday, Jan. 1

Martin Luther King Jr. Day
Monday, Jan. 19

Washington's Birthday, Presidents Day
Monday, Feb. 16

Memorial Day
Monday, May 25

Juneteenth National Independence Day
Friday, June 19

Independence Day
Saturday, July 4

Independence Day
Saturday, July 4

Labor Day
Monday, Sept. 7

Columbus Day
Monday, Oct. 12

Veterans Day
Wednesday, Nov. 11

Thanksgiving Day
Thursday, Nov. 26

Christmas Day
Friday, Dec. 25

Understanding returns and return codes

Return codes are used when the receiving bank is unable to post an entry to the Receiver's account and may return the entry back to the originating bank. Return codes provide the reason for the return. The financial institution will notify you of a return and then credit or debit the amount to your account. Return notification is typically provided to you by regular mail, email or online notification. Originators should receive return information within two banking days from the settlement date.

Return codes explain why funds are being returned.

Common return codes are:

- R01 Insufficient funds
- R02 Account closed
- R03 No account or unable to locate account
- R04 Invalid account number
- R06 Returned per ODFI's request
- R08 Payment stopped or stop payment on item
- R09 Uncollected funds
- R16 Account frozen
- R23 Credit entry refused by receiver
- R29 Corporate customer/accountholder advises not authorized

Unauthorized Return Codes are red flags for potential fraud

Originators should promptly investigate any entries returned with an unauthorized return code because these are red flags for potential fraud. The Receiving financial institution has up to 60 calendar days to return unauthorized entries. Common unauthorized return codes are:

- R05 Unauthorized debit to a consumer account using a corporate SEC code
- R07 Authorization revoked by a consumer accountholder
- R10 Customer/accountholder advises not authorized
- R11 Customer/accountholder advises entry not in accordance with the terms of the authorization

Re-initiating a returned item – RETRY PYMT

The only transactions that can be re-presented for settlement are:

- Those returned for Insufficient Funds or Uncollected Funds. There is a limit of two re-presentments within 180 days of the original entry date.
- A transaction that was returned for Stop Payment, if re-presenting it must be approved by the receiving party.

When re-initiating a returned item, RETRY PYMT in all capital letters is required in the company entry description field. Identical content is required in the following fields: company, name, company ID and amount. Modifications to other fields are permitted, but only to those necessary to correct an administrative error made during processing.

Reversals

Reversals are defined as a credit or debit entry that reverses an erroneous entry. If an Originator creates erroneous ACH entries or files, corrections may be made by initiating reversing entries or files. An erroneous entry or file is defined as:

- A duplicate of an entry previously initiated by the originator or ODFI
- Orders payment to or from receiver not intended to be credited or debited
- Orders payment in a dollar amount different then was intended

Reversals are requests

Reversals aren't mandatory transactions for the receiving financial institution, and they don't guarantee you will recover any funds. Receiving financial institutions don't have to put themselves in a negative position, such as overdrawing the receiver's account, to process a reversal. Reversals may be returned by the receiving institution.

The following must be present when submitting a reversal:

- REVERSAL must be in all capital letters in the description field of the company batch header record
- Originated within five banking days following settlement date of the erroneous entry
- Will need to build a new batch record
- Change the transaction codes to offset entries, for example debits reverse credits
- The effective date should be the same date as the original entry/file date for future dated files
- Notify the receiver of the reversal by the settlement date. In the case of an erroneous file, transmit a correcting file with the reversing file

We recommend that Originators use an authorization agreement with their Receivers that states they are authorized to debit/reverse any entries made in error. This is good business practice and will help with any disputes in the future.

Understanding your role regarding the security of non–public personal information

The Nacha Operating Rules require that each Originator and third–party sender must have policies and procedures in place regarding the initiation, processing and the storage of personal, non-public information, entries and files. Your security policies and procedures should accomplish the following requirements:

- Protect the confidentiality and integrity of the personal, non–public information, including financial information that you have on file, and the file information itself, until destruction. Other non–public information you may have on file includes EIN or tax ID numbers, dates of birth, social security numbers and addresses.
- Protect against anticipated threats and/or hazards that would threaten the security of the protected information until its destruction.
- Protect against the unauthorized use of that protected information which could cause harm to that individual and/or business.
- Security policies and procedures should be reviewed on an annual basis, or more frequently depending on your business needs. Check out **this guide** to help create your security incident response procedures.

Office of Foreign Asset Control

Originators must comply with Office of Foreign Asset Control requirements

You're required to check payees/ACH recipients against OFAC compliance checklists. OFAC checklists contain lists of countries, groups and individuals with which U.S. companies aren't permitted to send or receive funds.

It's against the law to send debit or credit entries to OFAC-blocked entities. You can check the OFAC SDN list **here**.

Notification of change

If the information on a transaction you originated is incorrect, you may receive a non-dollar correction transaction called a notification of change. It specifies information such as:

- Correct account number
- Correct routing/transit number
- Correct account type, like checking and/or savings

For example, if a receiving bank, also called receiving depository financial institution, has been through a merger, it may send you a NOC to provide new information that should be included on future transactions you originate.

The financial institution will notify you of any NOCs received. Changes need to be made before originating any further transactions to the same account. This is important to avoid disruption of payments or fines for uncorrected information which your financial institution may pass on to you. Following the NOC process, the receiving bank ensures that the information provided on future ACH transactions will be correct. By complying with the NOC, your business can originate from future transactions without having to obtain a new authorization.

Common NOC codes:

- C01 Incorrect bank account number
- C02 Incorrect routing/transit number
- C03 Incorrect routing/transit number and bank account number
- C05 Incorrect transaction code
- C06 Incorrect bank account number and transaction code
- C07 Incorrect routing/transit number, bank account number and transaction code

Authorizations

As an Originator, you're required to adhere to certain rules and agreements when initiating ACH transactions. An authorization is a document that is received by the Originator from the Receiver which authorizes the Originator to initiate a transaction on behalf of the Receiver.

- Consumer authorizations must be written and signed or similarly authenticated by the receiver.
- The receiver must also receive a copy of the written authorization.
- The terms of authorization must be clearly stated and understandable.
- Must contain instructions for termination.
- Originators are required to retain the authorization for two years from the termination or the revocation of the authorization.
- You must obtain authorization from a customer when making a one-time or recurring ACH debit and must indicate very clearly to the customer that they are authorizing a one-time or recurring ACH debit.
- You must take reasonable steps to ensure customers' routing numbers are valid.
- You must take steps to verify a customer's identity, without regard to whether a transaction is authorized online or by phone.
- You must be vigilant about possible fraud and do whatever is commercially reasonable to ensure the ACH transactions you initiate are not fraudulent.
- Ensure that you cancel a subscription promptly and stop making debits if a customer asks to cancel.

Standard Entry Class code

A Standard Entry Class code is a mandatory three-character code that's used in all batches to identify the types of entries within a batch.

Only one SEC code may be used for each batch of entries. If you have both consumer and business receivers, the entries will need to be split into separate batches, one for consumer Receivers, and one for corporate or business Receivers. If an incorrect SEC code is used for a batch, you will be subject to additional return risk exposure and the potential for monetary fines assessed by Nacha through the National System of Fines.

For example, if a batch of entries is sent to corporate or business receivers using the Pre-arranged Payment or Debit SEC code, debit entries may be returned for up to 60 days, and you must have an authorization.

Ensuring you're using the correct SEC code helps limit your liability for return entries and helps you avoid fines that may be assessed for using the improper SEC code. The most used SEC codes are:

PPD — Pre-arranged Payment or Debit

- For business-to-business consumer use only
- Most used for direct deposit
- Written authorization from the Receiver must be on file if you're debiting their account

CCD — Cash Concentration or Disbursement

- For business-to-business use only
- Can be used for moving funds between a business's own accounts at different institutions
- Used for payments or debits to other businesses
- Agreements are handled by contract authorization between companies

You can't combine different recipient types like consumers and businesses within a single batch. Different SEC codes are required based on the recipient type.

For example, you can't generate an ACH batch that contains employees for weekly payroll and businesses you're paying for invoices or other payment needs. You would need to originate one PPD batch containing all the employee transactions, and one CCD batch containing all the B2B transactions.

Company name

To ensure clear identification of the source of an ACH transaction, the Rules contain specific requirements with respect to how an Originator must identify itself within an ACH record. The Rules require the Originator to populate the Company Name field with the name by which it is known and readily recognized by the Receiver. This name could be the Originator's doing business as name or trading as name.

The inclusion of a readily recognizable Originator name ensures that the Receiver can identify a transaction appearing on their periodic statement. The clear identification of the Originator of an ACH transaction improves overall network quality by reducing the number of unrecognized entries requiring investigation and possible returns.

Fraud corner

Spotting and avoiding phishing and quishing scams

The world is in a constant state of communication. Between emails, texts and phone calls we receive a countless number of messages each day. Most of these are legitimate, but others are cleverly disguised to trick people into giving up their personal or financial information. Here's how to spot and avoid quishing and phishing scams.

Phishing for information

Phishing is where criminals send emails to "fish" for sensitive information like passwords, bank account numbers or debit card details. These messages often mimic legitimate companies or people you know or work with to create a sense of urgency. The context of the email may claim you need to update payment information. It may say you need to confirm personal or financial information. The email may include an invoice you don't recognize with a link for a non-traditional way to pay. It might also contain malicious links or attachments that lead to fake websites. At first glance, these emails look real, but odds are they're not.

Here are some common signs an email could be a scam:

- Unusual email address
- Unexpected messages requesting money, log-in credentials or sensitive information
- Suspicious links
- Generic references or greetings
- Misspelled words or messages with poor grammar

The hidden threat of quishing

Quick response codes, more commonly known as QR codes, are 2-D black and white matrix codes that store data which can be scanned with a camera or code reader application. They're widely used to store data such as URLs, product details or contact information. However, they can also be used by malicious actors to trick people into giving them their personal and financial information.

Quishing or QR phishing is the use of a QR code to redirect a user to a malicious site or link to gain access to the user's device or personal information. Tactics may include overlaying legitimate QR codes with malicious ones to trick users or relying on traditional phishing tactics such as a too-good-to-be-true deal with murky or falsified details.

Once the user clicks on the malicious link, they may be prompted to download malware or other harmful software. This can compromise the device and expose sensitive data such as banking credentials, browser history or other mobile activity.

Protecting yourself from quishing and phishing scams

Whether through a QR code, an email or a text message, bad actors use a variety of communication methods to trick people into sharing their personal or financial information.

Here are some tips to protect yourself:

- Look out for typos and poor grammar

- Watch out for a false sense of urgency
- Avoid unusual requests or payment methods
- Don't click suspicious links
- Inspect QR codes before scanning to check for tampering or overlays

What are the fraud risks for ACH?

Fraud challenges all participants in the ACH Network. Originators must remain vigilant to prevent and defend against fraud risk. There are certain common fraud schemes which you should be aware of. In one fraud scheme, fraudsters hack into an Originator's computer system using compromised user IDs and passwords and originate ACH credits to mule accounts created for the express purpose of committing fraud. Those accounts are then emptied and abandoned. The true Originator's account, your account, is debited for the invalid origination file. The credits are usually irretrievable by the time the fraud is discovered. The originator's credentials may have been compromised by an insider within the organization or stolen through key loggers or Trojan Horse programs on the compromised computer.

Due to the risk this type of fraud presents, it's essential that all computer equipment your company uses to operate treasury management and ACH Origination applications is regularly updated and patched for security vulnerabilities, including use of and updates to firewall, virus protection, anti-malware protection and anti-spam protection.

What is website spoofing?

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoofed websites are typically made to look exactly like a legitimate website published by a trusted organization.

To prevent fraud related to website spoofing:

- Pay attention to the web address of websites. A website may look legitimate, but the URL may have a variation in spelling or use a slightly different domain name.
- If you're suspicious of a website, close it and contact the company directly.
- Don't click links on social networking sites, pop-up windows or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to websites using a secure connection. Verify the web address begins with https:// rather than just http://.
- Avoid using websites for which your browser displays certificate errors or warnings.

Federal Reserve FraudClassifier model

The Federal Reserve worked with the payments industry to create the FraudClassifier™ model to help organizations classify fraud consistently. Nacha participated in the development of the FraudClassifier model and encourages the model's use. The model supports a common fraud language across payment types and fraud methods that can help all parties work together to identify and fight fraud. Applying the model across organizations and the industry ensures greater consistency in fraud classification, more robust information and better fraud tracking.

For additional information on the FraudClassifer model, visit the Federal Reserve's **website**.

Common credit-push ACH fraud schemes

It's critical for Originators to understand the nature of evolving fraud schemes and adopt appropriate risk control measures to combat them. According to Nacha, the most common ACH fraud schemes are business email compromise, vendor impersonation fraud, payroll impersonation fraud and account takeover fraud.

Business email compromise schemes

Business email compromise schemes occur when the legitimate email account of a business officer is either compromised or impersonated and used to order or request the transfer of funds. The employee transfers funds to the fraudster believing the order was from a reputable company email address owned by an officer with authority to make those orders. Business email compromise is classified as relationship and trust fraud by the Federal Reserve's FraudClassifier model because an authorized party was manipulated into initiating a payment.

Vendor impersonation fraud

Vendor impersonation fraud occurs when a business, public sector agency or organization receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The fraudster is paid by the business, agency or organization when the real contractor submits an invoice for work done or goods sold. Public sector organizations are frequently targeted because contract information is often in the public record. Vendor impersonation fraud is classified as relationship and trust fraud by the Federal Reserve's FraudClassifier model because an authorized party was manipulated into initiating a payment.

Payroll impersonation fraud

Payroll impersonation fraud targets employees and human resources departments. A fraudster will impersonate an employee and contact the HR department directly or through the employer's payroll portal using stolen credentials. The fraudster requests to change the account where the employee's regular payroll is deposited. Once updated, the employer pays the fraudster rather than the employee. Payroll impersonation fraud is classified as compromised credentials or impersonated authorized party depending on whether the fraudster uses stolen credentials to access the employer's HR portal or impersonates the employee when contacting the employer's HR department.

Account takeover fraud

Account takeover fraud occurs when a fraudster obtains the credentials of a consumer or a business bank account and pushes credits to their own accounts. The fraudster is active in the victim's online bank account, knows the account balances and can quickly deplete entire accounts. Account takeover fraud is classified as compromised credentials because an unauthorized party initiates payment using stolen credentials.

For additional information on cyber fraud, visit **Nacha's website**.

ACH RETURNS

An ACH Return is an ACH Entry that the RDFI is unable to post for reasons defined by the Return codes listed in the table below. More information on these Return reason codes can be found in the 2026 *Nacha Operating Rules & Guidelines* starting on page OR137.

RETURN CODE	DESCRIPTION	ENTRY TYPE	RETURN TIME FRAME	ACTION BY ORIGINATOR
R01	INSUFFICIENT FUNDS - Available and/or cash reserve balance not sufficient to cover amount of debit Entry.	ALL	2 Banking Bays	Originator may reinitiate the ACH Entry for a total of 3 presentments within 180 days of the Settlement Date of the original Entry for the same amount.
R02	ACCOUNT CLOSED – Previously active account has been closed.	ALL	2 Banking Days	Originator must stop initiation of Entries. Contact Receiver to obtain authorization for another account.
R03	NO ACCOUNT / Unable to Locate Account– Account number structure is valid, but the account number does not correspond to the individual identified in the Entry, or the account number designated is not an existing account.	ALL	2 Banking Days	Originator must stop initiation of Entries. Contact Receiver to obtain authorization for another account.
R04	INVALID ACCOUNT – Account number structure is not valid.	ALL	2 Banking Days	Originator must stop initiation of Entries until account number/structure is corrected.
R05	UNAUTHORIZED DEBIT TO CONSUMER ACCOUNT USING CORPORATE SEC CODE – A corporate Entry was transmitted to a consumer account that was not authorized.	CCD, CTX	60 Calendar Days	Originator must stop initiation of Entries. If a valid authorization exists, the Originator may have recourse outside the ACH Network.
R06	ODFI REQUEST FOR RETURN – ODFI has requested that the RDFI return an Entry.	ALL	Undefined	Originator must accept requested return.
R07	AUTHORIZATION REVOKED – The RDFI's customer revoked the authorization previously provided to the Originator for this debit Entry.	PPD, POS, TEL, WEB, IAT	60 Calendar Days	Originator must stop initiation of Entries until new consumer authorization is obtained. Depending upon the terms of the original authorization, the Originator may have recourse for collection outside the ACH Network.
R08	PAYMENT STOPPED – The Receiver has placed a stop payment order.	ALL	2 Banking Days	Originator must contact the Receiver to identify the reason for the Stop Payment and must stop initiation of the Entries until they receive instruction from the Receiver.
Ro9	UNCOLLECTED FUNDS – Sufficient ledger balance exists, to satisfy the dollar value of the transaction, but the available balance is below the dollar value of the debit Entry.	ALL	2 Banking Days	Originator may reinitiate the ACH Entry for a total of 3 presentments within 180 days of the Settlement Date of the original Entry and for the same dollar amount.
R10	CUSTOMER ADVISES ORIGINATOR IS NOT KNOWN TO RECEIVER /OR ORIGINATOR IS NOT AUTHORIZED BY THE RECEIVER TO DEBIT THE RECEIVERS ACCOUNT. - The RDFI has been notified by the Receiver that the Entry is unauthorized, improper or ineligible.	ARC, BOC, IAT, POP, POS, PPD TEL, WEB	60 Calendar Days	Originator must stop initiation of Entries. If a valid authorization exists, the Originator may have recourse outside the ACH Network.
R11	CUSTOMER ADVISES ENTRY NOT IN ACCORDANCE WITH THE TERMS OF THE AUTHOIRZATION. Transaction was incomplete, the amount debited was different, Debited earlier than authorized, Source document ineligible, Improperly reinitiated debit entry.	ARC, BOC, IAT, POP, POS, PPD TEL, WEB	60 Calendar Days	Originator would be permitted to correct the underlying error, if possible and, submit a new Entry without being required to obtain a new authorization. The new Entry must be Originated within 60 days of the Settlement Date of the R11 Return Entry.
R12	ACCOUNT SOLD TO ANOTHER DFI – A financial institution received an Entry to an account that was sold to another financial institution.	ALL	2 Banking Days	Originator must stop initiation of Entries and obtain correct routing number information for initiation of subsequent Entries.

ACH RETURNS

RETURN CODE	DESCRIPTION	ENTRY TYPE	RETURN TIME FRAME	ACTION BY ORIGINATOR
R16	ACCOUNT FROZEN/ENTRY RETURNED PER OFAC INSTRUCTION – 1) Access to the account is restricted due to specific action taken by the RDFI or by legal action or 2) OFAC has instructed the RDFI or Gateway to return the Entry.	ALL	2 Banking Days	Originator must stop initiation of Entries. Terms of authorization may offer recourse outside the ACH Network.
R17	File Record Edit Criteria/Entry with Invalid Account Number Initiated Under Questionable Circumstances.	ALL	2 Banking Days	Originator must identify and correct errors prior to initiation of further Entries. If the addenda field lists "Questionable" on an Entry that contains an invalid account number, it is believed by the RDFI to have been initiated under questionable circumstances.
R20	NON-TRANSACTION ACCOUNT – An Entry was transmitted to an account to which transactions are prohibited or limited.	ALL	2 Banking Days	Originator must stop initiation of Entries.
R23	CREDIT ENTRY DECLINED BY RECEIVER– Any credit Entry that is declined by the Receiver may be returned by the RDFI	ALL	2 Banking Days (after Receiver notifies RDFI)	Originator must obtain Receiver authorization prior to reinitiating the Entry.
R24	DUPLICATE ENTRY- The trace number, date, dollar amount, and/or other data matches another transaction.	ALL	2 Banking Days	If the Entry is duplicated, Originator should accept the return. If the Entry has already been reversed, Originator should contact their Financial Institution to determine a solution.
R29	CORPORATE CUSTOMER ADVISES NOT AUTHORIZED – RDFI has been notified by the Receiver that a specific Entry has not been authorized.	ALL	2 Banking Days	Originator must stop initiation of Entries until subsequent authorization has been obtained. If a valid authorization exists, the Originator may have recourse outside the ACH Network.
R31	PERMISSIBLE RETURN ENTRY – RDFI has received permission from the ODFI to transmit a late return.	CCD, CTX	Negotiated	Originator must accept return as agreed upon with RDFI. If the Originator or ODFI has not given permission for the untimely return, the return may be dishonored.
R37	SOURCE DOCUMENT PRESENTED FOR PAYMENT – The source document to which an ARC, BOC or POP Entry relates has been presented for payment.	ARC, BOC, POP	60 Calendar Days	Originator must accept return.
R38	STOP PAYMENT OF SOURCE DOCUMENT- A stop payment has been placed on the source document to which the Entry relates.	ARC, BOC, IAT*	60 Calendar Days	Originator must accept the return.
R39	IMPROPER SOURCE DOCUMENT – The RDFI determines the source document used is not an eligible item or the source document to which the Entry relates has been presented for payment.	ARC, BOC, IAT*, POP	2 Banking Days	Originator must accept the return.
R50	STATE LAW AFFECTING RCK ACCEPTANCE – RDFI is located in a state that has not adopted Revised Article 4 of the UCC or RDFI is located in a state that requires all canceled checks to be returned to the Receiver.	RCK	2 Banking Days	Originator must stop initiation of Entries.
R51	ITEM RELATED IS INELIGBLE or IMPROPER - notice not provided, signatures not genuine, item altered or amount of RCK not accurately obtained from the item.	RCK	60 Calendar Days	Originator must accept the return. Originator may attempt collection of item outside the ACH Network.
R52	*STOP PAYMENT ON ITEM – Stop Payment has been placed on an item to which the RCK Entry relates.*	*RCK*	60 Calendar Days	Originator must accept the return.

**IAT Entries that have a secondary SEC Code of ARC or BOC*

NOCs

(NOTIFICATION OF CHANGE)

A Notification of Change (NOC) is a non-dollar Entry transmitted by an RDFI to notify you that information contained within an Entry is erroneous and/or has become outdated and must be changed.

The *ACH Rules* require your company to make the requested changes within 6 banking days of the receipt of the NOC or prior to the initiation of another ACH Entry. More information on these NOC codes can be found in the 2026 Nacha Operating Rules & Guidelines starting on page OR180.

NOC CODE	DESCRIPTION	ACTION BY ORIGINATOR
C01	Incorrect Account Number.	Change the Receiver's account number record.
Co2	Incorrect Routing Number.	Change the Receiver's Financial Institution routing number.
C03	Incorrect Routing Number & Incorrect Account Number.	Change the Receiver's Financial Institution routing number & account number.
C05	Incorrect Transaction Code.	Change the two-digit transaction code.
C06	Incorrect Account Number & Incorrect Transaction Code.	Change the Receiver's account number and transaction code.
C07	Incorrect Routing Number, Account number & Transaction Code.	Change the Receiver's financial institution routing number, account number, and transaction code
C09	Incorrect Individual Identification Number.	Change the Individual ID number.
C13	Addenda Format Error.	Review the formatting in the Addenda Record that accompanied the original Entry Detail Record to determine errors and make corrections using only ANSI standards or Nacha endorsed banking conventions.
C14	Incorrect SEC Code for Out bound International Payment	The RDFI/Gateway has identified the Entry as an Outbound international payment and is requesting that future Entry be identified as IAT Entries.

Failure to respond to NOCs may result in fines to your FI according to the *Nacha Rules*

TRANSACTION CODES

Transaction Codes – Identify the various types of debit and credit Entries, pages OR135-OR136

Demand (Checking) Credits		Savings Credits		Financial Institution General Ledger Credits	
Tran Code	Description	Tran Code	Description	Tran Code	Description
21	Notification of Change or Return	31	Notification of Change or Return	41	Notification of Change or Return
22	Deposit	32	Deposit	42	Deposit
23	Prenotification	33	Prenotification	43	Prenotification
24	Zero dollar with remittance data	34	Zero dollar with remittance data	44	Zero dollar with remittance data

Demand (Checking) Debits		Savings Debits		Financial Institution General Ledger Debits	
Tran Code	Description	Tran Code	Description	Tran Code	Description
26	Notification of Change or Return	36	Notification of Change or Return	46	Notification of Change or Return
27	Payment	37	Payment	47	Payment
28	Prenotification	38	Prenotification	48	Prenotification
29	Zero dollar with remittance data	39	Zero dollar with remittance data	49	Zero dollar with remittance data

SEC CODE REQUIREMENTS

A Standard Entry Class (SEC) Code is a three-character code that identifies the type of Entry. There are specific requirements for each SEC code. Refer to Appendix Three of the 2026 *Nacha Operating Rules & Guidelines*, pages OR84 – OR112 for specific formatting requirements.

SEC CODES	Description	DEBIT/ CREDIT	CONSUMER/ CORPORATE	AUTHORIZATION REQUIREMENT
ARC- Accounts Receivable Entry	Check conversion Entry used to convert checks received via the U.S. mail, drop box, or in person for payment of a bill at a manned location	Debit	Consumer/ Corporate	Notification
BOC- Back Office Conversion	Check conversion Entry used to convert checks at point –of- sale or a manned bill payment location.	Debit	Consumer/ Corporate	Notification
CCD- Corporate Credit or Debit	Corporate to Corporate transactions	Credit or Debit	Corporate	Agreement
CTX- Corporate Trade Exchange	Corporate to Corporate transactions with payment related remittance information.	Credit or Debit	Corporate	Agreement
IAT- International ACH Transactions	The code that identifies an Entry that is part of a payment transaction involving a Financial Agency's office that is not located in the territorial jurisdiction of the United States.	Credit or Debit	Consumer/ Corporate	Consumer credit Entries - Oral or similarly authenticated; Consumer Debit Entries – written Corporate Entries – agreement
POP- Point of Purchase	Check conversion Entry used to convert checks received at the point-of-purchase or manned bill payment location	Debit	Consumer/ Corporate	Notification and Written
PPD- Prearranged Payment and Deposit Entry	A credit or debit Entry initiated by an organization to a consumer account of a Receiver based on a standing or a Single-Entry authorization from the Receiver. (Examples; Payroll, expense reimbursements, or bill payment such as utility or insurance).	Credit or Debit	Consumer	Credit – Written, Oral or Similarly authenticated. Debit – Written or Similarly Authenticated
RCK- Re-presented Check Entry	Check conversion Entry used to collect funds via the ACH Network for checks returned insufficient or uncollected funds.	Debit	Consumer	Notification
TEL- Telephone Initiated Entry	ACH Entry initiated by an Originator pursuant to an oral authorization obtained via the telephone	Debit	Consumer	Oral (must be recorded or written notice sent prior to Settlement Date)
WEB Debit - Internet Initiated/Mobile Entry	ACH Entry initiated pursuant to an authorization obtained via the Internet or Wireless Network.	Debit	Consumer	Similarly Authenticated (Examples: Digital Signature, shared secrets, biometrics etc.)

- You are authorized to use the SEC Codes in your agreement, if you wish to use other codes or confirm your authorized codes, please contact Midstates Bank and request Cash Management Team at (888)710-9070 or e-mail CashManagement@msbna.com .

Data Security, protecting personal information.

The *Nacha Operating Rules ("Rules")* require that Financial Institutions conducting ACH transactions employ a "security framework" aimed at protecting the security and integrity of certain ACH data throughout its lifecycle. One element of that security framework is the requirement that Financial Institutions require Originators to establish, implement and, as appropriate, update security policies, procedures and systems related to the initiation, processing and storage of ACH Entries and the related "Protected Information."

Protected Information is defined as "the non-public personal information, including financial information, of a natural person used to create, or contained within, an ACH Entry and any related Addenda Record." This would include your customers' account number or Social Security Number.

According to the Federal Trade Commission, there are five principles to protecting this information.

- Take stock.
  - Know what personal information you have in your files and on your computers.
- Scale down.
  - Keep only what you need for your business.
- Lock it.
  - Protect the information that you keep. The *Rules* say you must use a commercially reasonable method to encrypt ACH files you send to [financial institution].
  - Lock up any paperwork that contains customer data at your location.
- Pitch it.
  - Properly dispose of what you no longer need. Do not just throw the information in a garbage can.
- Plan ahead.
  - Create a plan to respond to security incidents.

Other tips as you create an ACH File or Entry

- If you send a Prenotification Entry, you must wait at least three business days before you send the live dollar Entry.
- You must not send both the Prenotification and the live dollar Entry on the same day.
- Make sure the name you use for your company is easily recognizable to the customer.
- Do not use Midstates Bank's name.
- If you have to abbreviate your name, make sure it is understandable to the customer. This is what they will see on their bank statement.

For in-depth information please refer to the Nacha Operating Rules & Guidelines or contact your financial institution. The words us and we refer to the Financial Institution and the words you and your refer to the Originator.

Authorization

You must obtain the Receiver's authorization which must be signed or similarly authenticated by the consumer.

- You must provide a copy of the authorization to the Receiver.

  The authorization must:

  1) Be readily identifiable as an ACH authorization.
  2) Have clear and readily understandable terms.
  3) Provide that the Receiver may revoke the authorization only by notifying you in the time and manner specified in the authorization.
- The authorization must be kept for two years following the termination or revocation of the authorization.
- If a copy of an authorization is requested by us, you must supply it so that we can respond to RDFI's (Receiving Depository Financial Institution) request. We have 10 Banking Days to provide the RDFI with the Authorization.
- If the Entry is a recurring debit you are required to notify the Receiver of any changes in the date or dollar amount.
  - At least seven (7) calendar days prior of a change in the date (consumer and corporate).

  - At least ten (10) calendar days prior to the change in the dollar amount (consumer only), unless it is within the agreed upon amount. Refer to the *Nacha Operating Rules and Guidelines*, for clarification, or contact us at the number listed).
- The Receiver's (your customer/employee) Financial Institution's deposit tickets should not be used to obtain the Financial Institution's routing number. These most often have internal processing numbers.

Notification of Change (NOC)

- A NOC is a non-dollar Entry transmitted by a RDFI to notify you that information contained within an Entry is erroneous and/or has become outdated and *must* be changed.
- The *ACH Rules* require you, the company, to make the requested changes within 6 Banking Days of the receipt of the NOC or prior to the initiation of another ACH Entry.
- Failure by you to respond to NOCs may result in fines to your Financial Institution.
- Call Midstates Bank and request Cash Management Team at (888)710-9070 or e-mail CashManagement@msbna.com if you have any questions.

Origination File

*In this example we used the Standard Entry Class (SEC) codes PPD & CCD, others can be found in the *Nacha Operating Rules and Guidelines*

- Have you used the correct SEC Code for the File you are sending?
  - A Payroll File is a credit going to a Consumer account and should have the SEC code of PPD.
  - Collections of Utility Payments, Condo Association Fees or any debit from a consumer should use the SEC code of PPD.
  - Collection of Utility Payments from a Business/Corporation the SEC code should be CCD.
  - Credit or Debit from a Corporate to a Corporate the SEC code should be CCD.
  - If you are collecting payments for both Consumer and Corporate, they should be originated as two separate batches.
  - The CCD SEC code has a 2-Banking Day return time frame and the PPD SEC code has a 60 calendar-day return time frame.
- The Company Name Field should be populated with a name that is readily recognized by the Receiver of the Entry
- The Company Entry Description Field should provide the Receiver with a description of the purpose of the Entry, (i.e. Payroll, Condo Fee, Utility Pay).

Fraud Monitoring

Each non-consumer Originator must establish and implement risk-based processes and procedures reasonably intended to identify ACH entries initiated due to fraud. These parties must also review, at least annually, their processes and procedures and make any appropriate updates to address evolving risks.

Effective dates for compliance with this rule are based on annual ACH origination volume in 2023.

- Effective March 20, 2026 - Non-consumer Originators with an annual ACH origination volume that exceeds 6 million entries in 2023. (Page OR7 – OR8)
- Effective June 22, 2026 – All remaining non-consumer Originators must comply with the rule.

Prenotification (Prenote)

Prenotifications are non-dollar Entries used to verify that the account number and routing number information is valid.

- Prenotifications may be sent as soon as 3 banking days prior to the first live dollar Entry.
- If the Prenote does not contain a valid account number, or is otherwise un-processable, you will receive either:
  - a return Entry, or
  - NOC
- You must fix the incorrect information before sending the next live Entry.

Returned Entries

- An ACH return is an ACH Entry that the RDFI is unable to post for reasons defined by the return codes.
- The following return reason codes have to be returned within 2 Banking Days of receiving it. If you receive a return Entry with one of the following return reasons, with the exception of R01, you *must stop initiating* the Entries and contact the Receiver:
  - R01 - Insufficient Funds (see Reinitiaton of Return Entries)
  - Ro2 - Account Closed
  - R03 - No Account
  - R04 - Invalid Account
  - R08 - Payment Stopped (A stop payment may be for one, several or all future Entries. You may not reinitiate the returned Entry unless the reason for the return is remedied. Contact the customer to determine the intent of the return.)
  - R29- Corporate Customer Advises not Authorized
- The following return reason codes can be returned up to 60 calendar days later if they are associated with a consumer SEC code. If you receive a return with one of these return reasons you *must stop initiating* the Entries. If a valid authorization exists, you may have recourse outside the ACH Network. Keep in mind you could get these back as late as 60 calendar days after you first initiated them. A Consumer must complete a Written Statement of Unauthorized Debit (WSUD) form when requesting an Entry be returned for one of these reasons. You may request a copy of the WSUD from your Financial Institution.
  - R05 - Unauthorized Debit to a Consumer Account using Corporate SEC code
  - R07 - Authorization Revoked
  - R10 - Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receivers Account.
  - R11 - Customer Advised Entry Not in Accordance with the Terms of the Authorization
  - R37 - Source Document Presented for Payment
  - R51 – Item Related to RCK Entry is Ineligible or RCK Entry is Improper.

Reinitiation of Return Entries

- You may reinitiate an Entry that has been previously returned (*other than an RCK*) if:
  - The Entry was returned for insufficient or uncollected funds.
  - The Entry was returned as stop payment and reinitiation has been authorized by the Receiver.
  - Corrective action was taken to remedy the reason for the return (example R11).
- Entry must be reinitiated within 180 days of settlement of the original Entry.
- You must not reinitiate an Entry that has been returned for insufficient or uncollected funds more than two times following the return of the original Entry (for a total of three times).
- The Entry was returned as stop payment and reinitiation has been *separately* authorized by the Receiver.
- Originator must submit Reinitiated Entries as a separate batch that contains the word "RETRY PYMT" in the Company Entry Description field of the Company/Batch Header Record.

Reversals

- As an Originator you may reverse an erroneous or duplicate ACH Entry/File up to 5 Banking Days after the Settlement Date of the Entry/File.
  - Erroneous Entry – an Entry that (a) is a duplicate of an Entry previously initiated by the Originator or ODFI; (b) orders payment to or from a Receiver different than the Receiver intended to be credited or debited by the Originator; or (c) orders payment in a dollar amount different than was intended by the Originator.
- A reversal is *not a guarantee* the File will be reversed. If there are not sufficient funds in the Receiver's account when the reversal is received by the receiving Financial Institution the reversal can be returned back to you.

International ACH Transactions (IAT) Due Diligence

- Do any of your employees, retired employees or Receivers have a foreign address to which their funds may be transferred to a non-US Financial Institution? If so, contact your Financial Institution with this information.

ACH Check Conversion

The ACH network supports the conversion of check items into ACH debit transactions. There are four specific applications, each with its own Standard Entry Class (SEC) code, supported by the ACH network. The SEC codes include: Accounts Receivable (ARC) Entries, which are checks that are mailed in or dropped off, normally bill payments, that are converted to ACH debits; Point-of-Purchase (POP) Entries, which are checks converted right at the point-of- sale terminal (usually a cash register); Back Office Conversion (BOC) Entries, which are checks taken at the point-of-sale and converted after the fact; and finally Represented Check (RCK) Entries, which are checks that were first returned as NSF or for uncollected funds, converted to be re-presented electronically. With the exception of RCK Entries, the check used to gather the information needed to generate these Entries is considered a source document, not a check.

Eligible Source Document

An Eligible Source Document is a Check that is used as a source of information for ARC, BOC or POP Entries. To be used as a source of information, the Check must:

- Contain a pre-printed Check serial number
- Be in an amount of $25,000 of less
- Be completed and signed by the Receiver (Maker of the Check) (except for POP)
- Have a routing number, account number and Check serial number encoded in magnetic ink

An Eligible Source Document does not include:

- A Check the contains an Auxiliary On-Us Field in the MICR line
- A Check payable to a Person other than the Originator (You)
- A draft that does not contain the signature of the Receiver, including any "remotely created check" as that term is defined by Regulation CC
- A Check provided by a lender for purposes of accessing a credit card account, home equity line or other form of credit
- A Check drawn on an Investment company as that term is defined in the Investment Company Act of 1940
- An obligation of the Financial Institution (e.g., travelers check, cashier's check, official check, money order)
- A Check drawn on the Treasury of the United States, a Federal Reserve Bank, or a Federal Home Loan Home
- A Check drawn on a state or local government that is not payable through or at a Participating DFI
- A Check Payable in a medium other than United States currency

Fraud Advisory for **Businesses**: Corporate Account Take Over

This product was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Problem:
Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered[1].

N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole $465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR $50,000 CYBER HEIST

Computer Crooks Steal $100,000 from Ill. Town

FBI Investigating Theft of $500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

Figure 1: Recent news headlines from *The New York Times*, *The Washington Post*, *Computer World*, and *Krebs on Security*.

[1] Consumer accounts are subject to Federal Reserve Regulations E (12C.F.R. Part 205) which requires banks to provide reimbursement for certain losses. Regulation E does not apply to business accounts. Therefore, banks are not required to provide reimbursement for certain losses.

To obtain access to financial accounts, cyber criminals target employees– often senior executives or accounting and HR personnel[2]- and business partners[3] and cause the targeted individual to spread malicious software (or "malware") which in turn steals their personal information and log-in credentials. Once the account is compromised, the cyber criminal is able to electronically steal money from business accounts. Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and ACH payments, or initiate other changes to the account. In addition to targeting account information, cyber criminals also seek to gain customer lists and/or proprietary information - often through the spread of malware - that can also cause indirect losses and reputational damage to a business.

First identified in 2006, this fraud, known as "corporate account take over," has morphed in terms of the types of companies targeted and the technologies and techniques employed by cyber criminals. Where cyber criminals once attacked mostly large corporations, they have now begun to target municipalities, smaller businesses, and non-profit organizations. Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud. Educating all stakeholders (financial institutions, businesses and consumers) on how to identify and protect themselves against this activity is the first step to combating cyber criminal activity.

This advisory was created by financial institutions, industry trade associations, Federal law enforcement and regulatory agencies.[4] It is intended to make businesses aware of this issue, identify some examples of how the fraud may occur, and provide updated recommendations to businesses to protect themselves against it. The information contained in this advisory is intended to provide basic guidance and resources for businesses to learn about the evolving threats and to establish security processes specific to their needs. However, it is very important to note that as the cyber criminals change their techniques, businesses must continue to improve their knowledge of and security posture against these attacks. In addition, the tips and recommendations contained in this advisory may help reduce the likelihood of fraud, but they should not be expected to provide complete protection against these attacks.

How it's Done:

Cyber criminals employ various technological and non-technological methods to manipulate or trick victims into divulging personal or account information. Such techniques may include performing an action such as opening an email attachment, accepting a fake friend request on a social networking site, or visiting a legitimate, yet compromised, website that installs malware on their computer(s).

---

[2] *Any* employee is vulnerable to being targeted.

[3] Business partners can include, among other third parties, contractors and accountants.

[4] This advisory was created through a collaborative cross-industry effort to develop and distribute recommended practices to prevent, detect and respond to corporate and consumer account takeovers. Led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), contributors include more than 30 of the largest financial institutions in the U.S., industry associations including the American Bankers Association (ABA), NACHA - The Electronic Payments Association, BITS/The Financial Services Roundtable; and federal regulatory and law enforcement agencies. This advisory is an update to recommendations previously released in August 2009 by the FS-ISAC, FBI and NACHA and NACHA (Operations Bulletin) in December 2009.

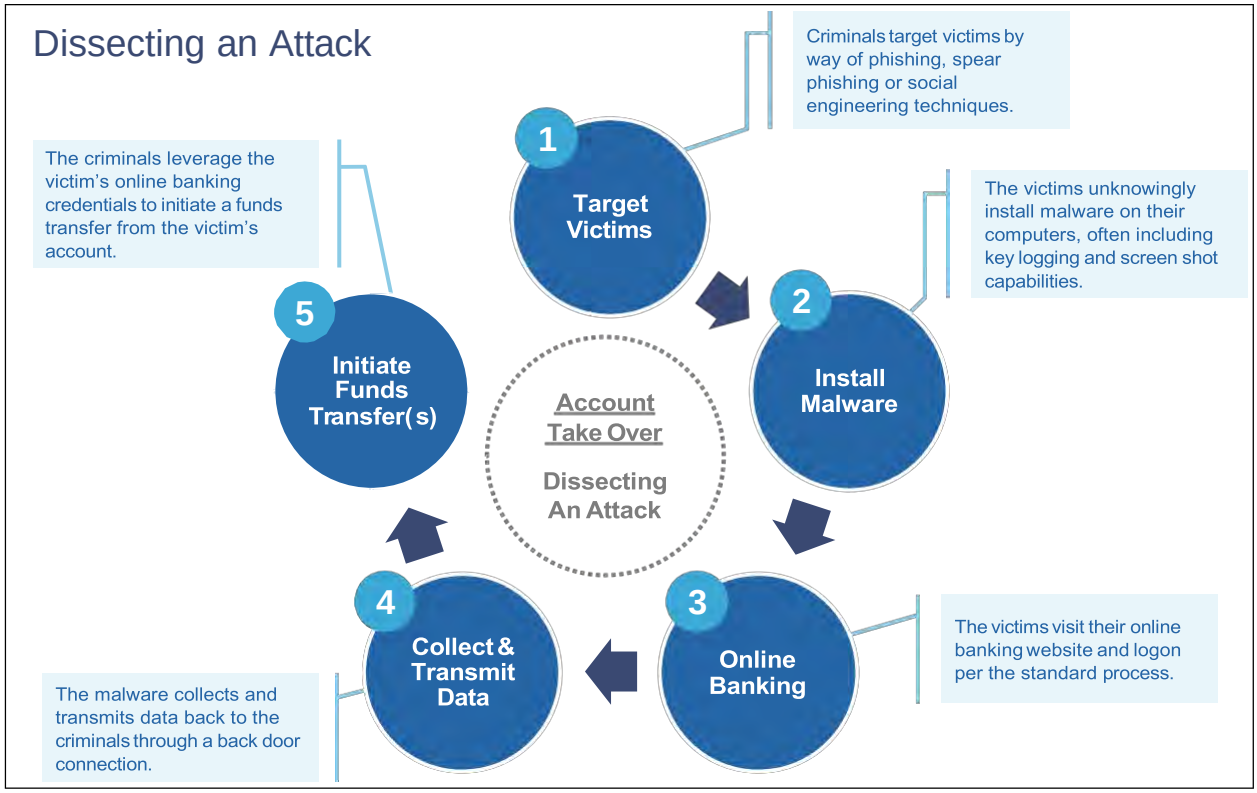

Figure 2: Dissecting An Account Take Over Attack

Cyber criminals will often "phish" for victims using mass emails, pop-up messages that appear on their computers, and/or the use of social networking and internet career sites[5]. For example, cyber criminals often send employees unsolicited emails that:

- Ask for personal or account information;
- Direct the employee to click on a malicious link provided in the email; and/or
- Contain attachments that are infected with malware.

Cyber criminals use various methods to trick employees into opening the attachment or clicking on the link, including:

- Disguising the email to look as though it's from a legitimate business. Often, these criminals will employ some type of scare tactic to entice the employee to open the email and/or provide account information. For example, cyber criminals have sent emails claiming to be from:
  1. UPS (e.g., "There has been a problem with your shipment.")
  2. Financial institutions (e.g., "There is a problem with your banking account.")
  3. Better Business Bureaus (e.g., "A complaint has been filed against you.")
  4. Court systems (e.g., "You have been served a subpoena.")

- Making the email appear to provide information regarding current events such as natural disasters, major sporting events, and celebrity news to entice people to open emails and click on links.

[5] Cyber criminals also use "vishing", which is soliciting victims over the phone or Voice over IP (VoIP).

- Using email addresses or other credentials stolen from company websites or victims, such as relatives, co-workers, friends, or executives and designing an email to look like it is from a trusted source to entice people to open emails and click on links.

The cyber criminal's goal is to get the employee to open the infected attachments or click on the link contained in the email and visit the nefarious website where hidden malware is often downloaded to the employee's computer. This malware allows the fraudster to "see" and track employee's activities across the business' internal network and on the Internet. This tracking may include visits to your financial institution and use of your online banking credentials used to access accounts (account information, log in, and passwords). Using this information, the fraudster can conduct unauthorized transactions that appear to be a legitimate transaction conducted by the company or employee.

How to Protect, Detect, and Respond

Protect

1. **Educate everyone on this type of fraud scheme**
    - Don't respond to or open attachments or click on links in unsolicited e-mails. If a message appears to be from your financial institution and requests account information, do not use any of the links provided. Contact the financial institution using the information provided upon account opening to determine if any action is needed. Financial institutions do not send customers e-mails asking for passwords, credit card numbers, or other sensitive information. Similarly, if you receive an email from an apparent legitimate source (such as the IRS, Better Business Bureau, Federal courts, UPS, etc.) contact the sender directly through other means to verify the authenticity. Be very wary of unsolicited or undesired email messages (also known as "spam") and the links contained in them.
    - Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.
    - Teach and require best practices for IT security. See #2, "Enhance the security of your computer and networks".

2. **Enhance the security of your computer and networks to protect against this fraud[6]**
    - Minimize the number of, and restrict the functions for, computer workstations and laptops that are used for online banking and payments. A workstation used for online banking should not be used for general web browsing, e-mailing, and social networking. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.
    - Do not leave computers with administrative privileges and/or computers with monetary functions unattended. Log/turn off and lock up computers when not in use.
    - Use/install and maintain spam filters.
    - Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software.
        - Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
    - Install routers and firewalls to prevent unauthorized access to your computer or network.
        - Change the default passwords on all network devices.
    - Install security updates to operating systems and all applications, as they become available. These updates may appear as weekly, monthly, or even daily for zero-day attacks.
    - Block pop-ups.

[6] See the "Resources" section for links to helpful and detailed tips on how to enhance your information technology (IT) security.

- As recommended by Microsoft for users more concerned about security, many variants of malware can be defeated by using simple configuration settings like enabling Microsoft Windows XP[7], Vista[8], and 7 Data Execution Prevention (DEP)[9] and disabling auto run commands[10]. You may also consider disabling JavaScript in Adobe Reader[11]. If these settings do not interfere with your normal business functions, it is recommended that these and other product settings be considered to protect against current and new malware for which security patches may not be available.
- Keep operating systems, browsers, and all other software and hardware up-to-date.
- Make regular backup copies of system files and work files.
- Encrypt sensitive folders with the operating system's native encryption capabilities. Preferably, use a whole disk encryption solution.
- Do not use public Internet access points (e.g., Internet cafes, public wi-fi hotspots (airports), etc.) to access accounts or personal information. If using such an access point, employ a Virtual Private Network (VPN)[12].
- Keep abreast of the continuous cyber threats that occur. See the Additional Resources section for recommendations on sites to bookmark.

3. **Enhance the security of your corporate banking processes and protocols**
   - Initiate ACH and wire transfer payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file from a different computer system. This helps ensure that one person does not have the access authority to perform both functions, add additional authority, or create a new user ID.
   - Talk to your financial institution about Positive Pay and other services such as SMS texting, call backs, and batch limits which help to protect companies against altered checks, counterfeit check fraud and unauthorized ACH transactions.
   - If, when logging into your account, you encounter a message that the system is unavailable, contact your financial institution immediately.

4. **Understand your responsibilities and liabilities**
   - Familiarize yourself with your institution's account agreement**.** Also be aware of your liability for fraud under the agreement and the Uniform Commercial Code (UCC), as adopted in the jurisdiction, as well as for your responsibilities set forth by the Payment Card Industry Data Security Standard (PCI DSS), should you accept credit cards. For more information, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Detect

5. **Monitor and reconcile accounts at least once a day**
   - Reviewing accounts regularly enhances the ability to quickly detect unauthorized activity and allows the business and the financial institution to take action to prevent or minimize losses.

6. **Discuss the options offered by your financial institution to help detect or prevent out-of-pattern activity (including both routine and red flag reporting for transaction activity).**

---

[7] How to configure memory protection in Windows XP SP2; http://technet.microsoft.com/en-us/library/cc700810.aspx
[8] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows-vista/Change-Data-Execution-Prevention-settings
[9] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows7/Change-Data-Execution-Prevention-settings
[10] How to disable the Autorun functionality in Windows: http://support.microsoft.com/kb/967715/
[11] Disabling JavaScript in Adobe Reader and Acrobat; http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html
[12] A VPN uses the public telecommunication infrastructure and the Internet to provide remote and secure access to an organization's network.

7. **Note any changes in the performance of your computer such as:**
    - A dramatic loss of speed.
    - Changes in the way things appear.
    - Computer locks up so the user is unable to perform any functions.
    - Unexpected rebooting or restarting of your computer.
    - An unexpected request for a one time password (or token) in the middle of an online session.
    - Unusual pop-up messages.
    - New or unexpected toolbars and/or icons.
    - Inability to shut down or restart.

8. **Pay attention to warnings**
    - Your anti-virus software should alert you to potential viruses. If you receive a warning message, contact your IT professional immediately.

9. **Be on the alert for rogue emails**
    - If someone says they received an email from you that you did not send, you probably have malware on your computer.
    - You can also check your email "outbox" to look for email that you did not send.

10. **Run regular virus and malware scans of your computer's hard drive**
    - This can usually be set to run automatically during non-peak hours.

Respond

11. **If you detect suspicious activity, immediately cease all online activity and remove any computer systems that may be compromised from the network.**
    - Disconnect the Ethernet cable and/or any other network connections (including wireless connections) to isolate the system from the network and prevent any unauthorized access.

12. **Make sure your employees know how and to whom to report suspicious activity to within your company and at your financial institution**

13. **Immediately contact your financial institution so that the following actions may be taken:**
    - Disable online access to accounts.
    - Change online banking passwords.
    - Open new account(s) as appropriate.
    - Request that the financial institution's agent review all recent transactions and electronic authorizations on the account. If suspicious active transactions are identified, cancel them immediately.
    - Ensure that no one has added any new payees, requested an address or phone number change, created any new user accounts, changed access to any existing user accounts, changed existing wire/ACH template profiles, changed PIN numbers or ordered new cards, checks or other account documents be sent to another address.

14. **Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident to the various agencies, financial institutions, and firms impacted**
    - Be sure to record the date, time, contact telephone number, person spoken to, instructions, and any relevant report or reference number.

15. **File a police report and provide the facts and circumstances surrounding the loss**
    - Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often help facilitate the filing of claims with insurance companies, financial institutions, and other establishments that may

be the recipient of fraudulent activity.

- The police report may result in a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender, and possibly recovering losses.
- Depending on the incident and the circumstance surrounding the loss, investigating officials may request specific data be recorded and some or all of the system's data may need to be preserved as potential evidence.
- In addition, you may choose to file a complaint online at www.ic3.gov. For substantial losses, contact your local FBI field office (http://www.fbi.gov/contact-us/field/field-offices), your local United States Secret Service field office

(http://www.secretservice.gov/field_offices.shtml), or the Secret Service's local Electronic Crimes Task Force (http://www.secretservice.gov/ectf.shtml).

16. Have a contingency plan to recover systems suspected of compromise

- The contingency plan should cover resolutions for a system infected by malware, data corruption, and catastrophic system/hardware failure. A recommended malware removal option is to reformat the hard drive, then reinstall the operating system and other software on the infected computer(s). There is no preservation of data using this method – all your data will be permanently erased. Do not take this step until you determine if a forensic analysis of the computer is needed. For additional recommendations on steps to take following a compromise, see the section "What if I am Compromised" on page 6 of the US CERT document, *Malware Threats and Mitigation Strategies* available at http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf

17. Consider whether other company or personal data may have been compromised

18. Report exposures to PCI DSS.

- If your business accepts credit cards, you are subject to compliance with the Payment Card Industry Data Security Standard (PCI DSS) and you may be required to report and investigate the incident, limit the exposure of the cardholder data, and report the incident to your card company. For more information, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Contact your financial institution for more information.

Additional Resources:

- Federal Trade Commission (FTC) website, "Computers& the Internet: Privacy and Security"[13] (includes OnGuard Online),
- Internet Crime Complaint Center (IC3)[14],
- Department of Homeland Security Cyber Report[15],
- National Cyber Security Alliance Stay Safe Online[16].
- Better Business Bureau- "Data Security Made Simple"[17]
- Microsoft Security Page[18]
- U.S. Chamber of Commerce's "Internet Security Essentials for Small Business"[19]

---

[13] http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm

[14] The IC3 is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA). For more information, see http://www.ic3.gov/default.aspx.

[15] http://www.cyber.st.dhs.gov/

[16] http://www.staysafeonline.org/

[17] http://www.bbb.org/data-security/

[18] http://www.microsoft.com/security/default.aspx

[19] This document is scheduled for release on October 26, 2010. Visit www.uschamber.com/cybersecurity for more information.