MAGIC WRIGHTER

Payment Solutions. Partnerships. Opportunities.

Financial Institution
Electronic Payment Services

Risk Management

Best Practices

ACH
&
Credit Card

Confidential Information

Revised: October 2023

Risk Management & Best Practices
Table of Contents

Risk Management & Best Practices
Table of Contents

Risk Management & Best Practices
Overview

Magic-Wrighter's business customer related products and services contain Risk Management, Risk Monitoring, and Risk Controls. These controls are considered Companion or Complementary controls that enhance the standard integrated risk controls.

Each service provides specific companion controls that are suitable for the service.

The following pages explain the Risk Management and *Best Practices* as they relate to each of Magic-Wrighter's products and services.

Your financial institution should consider incorporating the following *Risk Management* controls into your institution's overall Risk Management Program.

> Disclaimer: The *Risk Management & Best Practices* discussed within this document have been developed to work in conjunction with the products and services provided in the Magic-Wrighter suite of Electronic Payment Services. If your financial institution is not using the Magic-Wrighter suite of products and services, we recommend you obtain the Risk Management and Best Practices from your current vendor.

General Overview

Your financial institution should include NACHA, Reg E, State, and FFIEC Best Practices guidelines when using Magic-Wrighter's Complementary User Entity Controls.

It is important that your institution has a comprehensive risk management program that addresses subjects not found in the risk management, risk monitoring, and risk controls set forth in the suite of Magic-Wrighter's Complementary User Entity Controls.

Risk Management & Best Practices
Overview

(This page intentionally left blank)

Risk Management & Best Practices
Know Your Customer

Know Your Customer

Your financial institution is in the best position to "***know your customer***".

Knowing your customer is not limited to just their financial position. Because your institution may use some or all the Magic-Wrighter suite of products to electronically collect payments, disburse payroll direct deposits, and/or provide other electronic transfers of funds to your business customer, it is important that you know the characteristics of your client's company or organization.

These items include:

- What business are they in?
- Are they in good standing with the Better Business Bureau?
- Do they have sufficient cash-flow to support ACH services?
- What is their Dunn and Bradstreet rating?
- Are their financial statements in order?
- Have they filed the proper tax returns?
- Do they have outstanding liens?
- How long have they been in your community?
- Are the services requested in line with their business services?

NACHA Terminated Originator Database

NACHA provides a Terminated Originator Database to all financial institutions. The Terminated Originator Database is not a list of prohibited or disapproved Originators and Third-Party Senders but rather companies where a financial institution determined it was not in the institution's best interest to continue providing the business customer with ACH Origination services.

Your institution should utilize the information obtained from the NACHA Terminated Originator Database as part of your overall effort to evaluate new and current ACH Originators.

Your institution should independently perform due diligence to determine how this information will factor into your decision-making and monitoring processes.

Risk Management & Best Practices
Know Your Customer

(This page intentionally left blank)

Risk Management & Best Practices
Risk Management

Your financial institution has many options available that will reduce your risk exposure based on the service and type of transactions that are processed via the ACH network.

There is no single solution that will protect your financial institution 100% of the time. The key to best practices and risk mitigation is to use a combination of services that best suits the service that is offered and the type of client that has requested the service.

Market Factors

The following market factors should be considered for higher risk clients:

- Withhold funds sooner
- Require reverse wire transfers
- Limit usage of direct deposit
- Restrict funds to isolated accounts

Enhanced Due Diligence and Tactics

The following enhanced due diligence and activities should be considered for new clients:

- 2 years financial statements and tax returns
- Visit client's office
- Credit bureau review on owners
- 3 months of bank statements
- Google search
- Social media search
- Understand corporate structure and business model
- Owner guarantee of direct deposit of payroll exposure
- Establish individual client direct deposit payroll limits
- Reserve right to offset funds from related accounts
- Manage NSF aggressively
- Enforce one strike NSF policy
- Copy of driver's license
- Require tax service for direct deposit of payroll
- Evaluate your NSF return percentage at least annually

Risk Management & Best Practices
Risk Management

(This page intentionally left blank)

Risk Management & Best Practices
General Customer Setup

General Customer Setup

Before signing an ACH Origination service agreement with your business customer, your financial institution should collect several important items and perform a risk review and analysis on your customer's request for services.

Items to collect and review:

- Financial statements for the past two years
- Tax returns for the past two years
- Credit check
- Dunn and Bradstreet report
- Credit Committee review

After your financial institution has determined the company is an acceptable credit risk, you should complete the following items:

- Sign ACH Origination, Remote Deposit Capture, Treasury Management, or other agreement(s) created by your institution for the services requested by the customer
- Complete the company information form
- Review fee schedule with your customer
- Establish daily risk limit
- Complete required authorization forms for each service requested
- Complete the new customer check list

Risk Management & Best Practices
General Customer Setup

Batch Suspension

This feature is generally used for business customers requesting consumer-initiated online payments. In this environment, consumers are making payments 24x7, and establishing a pre-determined limit that would require the business customer to stop accepting online payments when the limit is reached is impractical.

To address this issue, a financial institution should establish a reasonable risk limit for business customers accepting online payments. During each end-of-day processing cycle, the actual payments to be processed are checked against the established limit(s). Should transactions exceed the pre-established limit, they are automatically suspended and, a suspended batch advisory email is sent to the financial institution.

The financial institution is responsible for determining the proper procedures required to release suspended transactions. This procedure usually includes a credit manager or other senior officer's approval.

Batch suspension can be used to suspend all activity for all business customers. This practice is usually performed when a financial institution's credit policy requires review of all transaction activity for specific or all business customers prior to releasing the transactions to the ACH payment network.

Note: This service is not automatically activated for your financial institution since many institutions use internal core vendor controls to manage customer risk. Contact Magic-Wrighter's customer support to activate automatic batch suspension for your customer and batch suspension training.

Risk Management & Best Practices
Payroll Direct Deposit

Initial Setup

Business customers requesting employee payroll direct deposit should complete the following forms prior to starting their direct deposit program:

Payroll Direct Deposit Debit Authorization – provides your financial institution with authorization to withdraw funds from the business customer's corporate account to offset the credits due to each employee.

Your financial institution must follow the NACHA rules and store this authorization for the complete time service is provided and a minimum of two years after termination of the authorization or service.

> Note: This form may not be required if your financial institution allows your business customer to transmit a balanced file where the total credits and total debits within the file are equal.

Payroll Processing – provides your institution with the description of the payroll, frequency to expect the payroll, and contact information. This information will allow your ACH department to establish a payroll transmission calendar. The calendar can be used to monitor expected employer payroll transmissions, allowing you to red flag unauthorized transmissions.

Employee Payroll Direct Deposit Authorization – NACHA requires all originators, in this case your business customer, to obtain permission to deposit payments into an employee's checking or savings account. Your institution should verify your business customer is using an authorization form that follows the NACHA authorization guidelines.

Verify with your business customer that they have obtained a signed copy from each employee requesting payroll direct deposit and that the company will store the forms in a safe place for a minimum period as outlined by NACHA rules.

Your business customer should be instructed to retain copies of deposit authorizations for a period of two years after employee termination.

Risk Management & Best Practices
Payroll Direct Deposit

Risk Exposure Assessment

Your financial institution's risk exposure can increase or decrease as risk variables are added or removed from the risk probability equation.

Example:

The NACHA rules state that once your institution has sent employee payroll direct deposit transactions to the ACH operator (typically the Federal Reserve Bank via Fed ACH or your direct ACH gateway), your financial institution has guaranteed the funds.

The NACHA rules also permit employee payroll direct deposit transactions to be transmitted by your institution to the ACH Network up to two (2) days in advance of the posting due date, but only allows your institution to transmit the offset payroll debit one day in advance.

Your institution should have a high confidence risk rating that, on the day the funds are debited from the business customer's corporate account, the fully collected funds will be available.

Customer Does Not Have a Corporate Account at Your Institution – when you allow a business to debit a corporate account located at another financial institution to cover the disbursement of funds, your financial institution will experience a higher degree of risk exposure, due to the fact that if payment is not received prior to the release of the deposits, your institution has guaranteed the funds to the ACH Network and you do not have offset funds in your possession.

Funds Deposited by Corporate Check – when your institution accepts a paper corporate check to offset the disbursed payments, your institution is accepting *uncollected funds*. This means that if there are insufficient funds in the corporate account or the account has been closed at the time the check clears, the RDFI will return the check, creating a risk exposure.

Risk Management & Best Practices
Payroll Direct Deposit

Risk Exposure Assessment (continued)

Funds Deposited by Wire Transfer – when wire transfers are used to offset the disbursed payments, your institution should verify the wire transfer has been completed prior to the release of the payment transactions to the ACH Network.

Funds Deposited by Cashier's Check – Cashier's checks should be validated prior to the release of payments to the ACH Network.

Funds Are Drawn from a Deposit Account Located at Your Institution - this practice provides a lesser degree of risk exposure than funds drawn on a foreign corporate account, but still needs consideration. The primary risk exposures are a) the funds in the offset corporate account are not collected funds, b) the company withdraws the funds between the time your institution releases the deposit payments and the day the offset debit is applied to the corporate account.

Offset Account Risk Exposure Mitigation

To mitigate your institution's risk exposure when releasing credit transactions to the ACH Network, your institution should consider the following:

- Establishing an ACH offset corporate account for each business where funds are deposited and offset funds for disbursed ACH credits are held.
- Prior to the release of ACH credit transactions to the ACH Network, verify collected funds are in the ACH offset corporate account.
- Establish a line of credit for the business sufficient to cover disbursed ACH credits on any given day.
- Place a hold on funds located in the business corporate account equal to the credits that are to be disbursed.

Risk Management & Best Practices
Payroll Direct Deposit

Establishing Risk Limit Exposures

The system allows your institution to establish a series of *risk limit exposures*. By using each of the following limits, liability exposure can be reduced.

Per Transaction – this option allows your institution to establish the maximum amount of a single deposit amount within a credit batch that will be accepted by your financial institution. When activated, the system will automatically reject a file that is transmitted by your business customer if a credit transaction exceeds the set amount.

Per Batch Limit – this option allows your financial institution to establish the maximum amount of a specific batch that will be accepted. When activated, the system will automatically reject a file that is transmitted by your business customer if the dollar amount of the batch transmitted exceeds the set limit.

When using the Per Batch Limit option, your institution must define each batch that will be accepted by your financial institution by assigning a specific company ID and batch description to each batch transmitted by your business customer.

Touch Tone Payroll Limit - establishes the maximum posting amount your financial institution will accept from your business customer when using the IVR (Interactive Voice Response) Touch Tone Payroll service to post their payroll transactions. When the total payroll amount exceeds the Touch Tone Payroll Limit, the business customer will be notified that they have exceeded their limit, via automatic notification, and that they should contact your financial institution. The payroll will not be accepted for posting. The customer may contact your institution and request their limit be increased.

Computer Transmission Limit – establishes the maximum amount that will be accepted by your institution in a single computer transmission from your business customer. If the transmission amount exceeds this limit, your business customer will be informed they have exceeded their computer transmission limit, via automatic notification, and that they should contact your financial institution. The computer transmission will not be accepted for posting. The business customer may contact your institution and request their limit be increased.

Risk Management & Best Practices
Payroll Direct Deposit

Establishing Risk Limit Exposures (continued)

Total Daily Limit – establishes the maximum dollar amount of transactions your financial institution will accept in a single day from a business customer. When determining if the customer is within their total daily limit, the system will combine all credit transactions posted by your business customer for the requested posting date. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on the Daily Risk Report. Upon review of the Daily Risk Report, you may contact your business customer informing them they have exceeded their risk limit. Your business customer may request their daily limit be increased.

Daily Risk Report - your institution should review the Daily Risk Report prior to transmitting files to your ACH Operator. When you determine a business customer's transmission should be cancelled, your institution will have the opportunity to remove the transactions from the file.

> Example: If you set the Total Credit Limit to $20,000 and your customer transmits a payroll for $12,000, a transfer of funds for $4,000 and a tax payment of $5,000, an Over Daily Limit message will be printed on your Daily Risk Report and show an over limit of $1,000.

48 Hour Limit - establishes the maximum file total your financial institution will accept in a 48-hour timeframe (two banking business days) from your business customer. The system will combine all credit transactions posted by your business customer during the last 48 hours. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer when they have exceeded their risk limit to discuss additional funding requirements.

10 Day Limit - establishes the maximum dollar amount your financial institution will accept in a ten (10) day period from your customer. The system will combine all credit transactions posted by your business customer during the last ten days. If the combined File Totals exceeds this limit, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer when they have exceeded their risk limit to discuss required additional funding requirements.

Risk Management & Best Practices
Payroll Direct Deposit

Establishing Risk Limit Exposures (continued)

30 Day Limit - establishes the maximum File Total your financial institution will accept in a thirty (30) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last thirty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your business customer when they have exceeded their limit.

60 Day Limit - establishes the maximum File Total your financial institution will accept in a sixty (60) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last sixty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your customer when they have exceeded their limit.

Restricting Transaction Type

Your financial institution may restrict the transaction types your business customer is permitted to originate.

If the business customer transmits a transaction type that has not been authorized by your financial institution, the file transmission will be rejected. Your business customer will receive a notification indicating that the transmission was rejected.

Risk Management & Best Practices
Payroll Direct Deposit

Establishing Risk Limit Exposures (continued)

Balanced File

This option allows your financial institution to require that your business customers transmit a balanced file (credit and debit dollar amounts are equal). When this option is activated, the system will not allow your business customer to transmit an out of balance file to your financial institution.

If your customer transmits an out of balance file, the transmission will be rejected. Your business customer will be notified that the transmission has been rejected.

You should not use this option if your internal banking system is expecting ACH files to be offset by a pre-loaded account number assigned to a specific business customer.

Offset Account Number

This feature is used in conjunction with the Balanced File option and Batch Authentication option.

This feature allows your financial institution to designate the predetermined corporate account(s) your business customer may debit when transmitting a payroll direct deposit batch.

Risk Management & Best Practices
Payroll Direct Deposit

(This page intentionally left blank)

Risk Management & Best Practices
State & Federal Tax Payments

Initial Setup

Business customers requesting the State and Federal tax payment service should complete the following forms prior to starting their State & Federal Tax Payments program:

State/Federal Tax Payments Debit Authorization – this will provide your financial institution with the authorization to withdraw funds from the customer's account to offset the credits sent to the government.

Your financial institution must follow the NACHA rules and store this authorization for the complete time service is provided, including two years after termination of the service.

Note: This form may not be required if your financial institution allows your business customer to transmit a balanced file where the total credits and total debits within the file are equal.

Tax Payment Processing Schedule – this will provide your institution with the description of tax payment(s), frequency to expect the payments, and customer contact information. This information will allow your ACH department to establish a tax payment transmission calendar. The calendar can be used to monitor expected tax payment transmissions, allowing you to red flag unauthorized transmissions.

Credit Authorization – your business customer should obtain authorization from the government to make electronic tax payments. Your institution should verify that your customer has obtained the proper authorization to prevent returned unauthorized credit payments from the government.

Risk Exposure Assessment

Your financial institution's risk exposure can be increased or decreased as risk variables are added or removed.

Example:

NACHA rules state that when your institution transmits a government tax payment to the ACH Operator (typically the Federal Reserve Bank via FedACH or your direct ACH gateway), your financial institution has guaranteed the funds.

Risk Management & Best Practices
State & Federal Tax Payments

Risk Exposure Assessment (continued)

To ensure payments are received by the government on the scheduled payment date, business customers will need to transmit payments at least one (1) day in advance of the posting due date.

Your institution is responsible for educating your customer of transmission deadlines and your institution's funding requirements.

Your institution should have a high degree of confidence that, on the day the funds are debited from the business customer's corporate account, fully collectable funds will be available.

Customer Does Not Have a Corporate Account at Your Institution – when you allow a business to debit a corporate account located at another financial institution to fund the disbursement of ACH credits, your financial institution may have a higher degree of risk exposure based to the fact that your institution has guaranteed the funds but you do not have the offset funds in your possession.

Funds Deposited by Corporate Check – when your institution accepts a paper corporate check drawn on a foreign financial institution for the offset of ACH credits, your institution may be accepting a higher risk exposure since the RDFI may decline the check.

To mitigate your institution's risk, you should consider establishing a line-of-credit, obtain collateral sufficient to cover disbursed funds while the check clears or use other methods that would guarantee the availability of funds when the check is presented to the receiving institution.

Funds Deposited by Wire Transfer – when wire transfers are used to offset the disbursed payments, your institution should verify the wire transfer has been completed prior to the release of the payment transactions to the ACH Network.

Funds Deposited by Cashier's Check – Cashier's checks should be validated prior to the release of payments to the ACH Network.

Risk Management & Best Practices
State & Federal Tax Payments

Risk Exposure Assessment (continued)

Funds Are Drawn from a Deposit Account Located at Your Institution - this practice provides a lesser degree of risk exposure than funds drawn from a foreign corporate account, but still needs consideration. The primary risk exposures are a) the funds in the offset corporate account are not collected funds, b) the company withdraws the funds between the time your institution releases the tax payments and the day the offset debit is applied to the corporate account.

To mitigate your institution's risk, consider establishing a business account and require your customer to fund the account with 'collected funds' and prohibit your customer from withdrawing funds from the account.

Offset Account Risk Exposure Mitigation

To mitigate your institution's risk exposure when releasing tax payment transactions to the ACH Network, your institution should consider the following:

- Establishing an ACH offset corporate account for each business where funds are deposited and offset funds for disbursed ACH credits are held.
- Prior to the release of ACH credit transactions to the ACH Network, verify collected funds are in the ACH offset corporate account.
- Establish a line of credit for the business sufficient to cover disbursed ACH credits on any given day.
- Place a hold on funds located in the business corporate account equal to the credits that are to be disbursed.

Establishing Risk Limit Exposures

The system allows your institution to establish a series of Risk Limit Exposures. By using each of the following limits, liability exposure can be reduced.

Per Transaction – this option allows your institution to establish the maximum amount allowed for a single transaction within a batch that will be accepted by your financial institution. When activated, the system will automatically reject a file that is transmitted by your business customer if a credit transaction exceeds the set amount.

Risk Management & Best Practices
State & Federal Tax Payments

Establishing Risk Limit Exposure (continued)

Per Batch Limit – this option allows your financial institution to establish the maximum amount of a specific batch that will be accepted. When activated, the system will automatically reject a file that is transmitted by your business customer if the dollar amount of the batch transmitted exceeds the set limit.

When using the Per Batch Limit option, your institution must define each batch that will be accepted by your financial institution by assigning a specific company ID and batch description to each batch transmitted by your business customer.

Touch Tone Tax Payment Limit - establishes the maximum posting amount your financial institution will accept from your business customer when using the IVR (Interactive Voice Response) Touch Tone Tax Payment service to post their tax payments. When the tax payment amount exceeds the Touch Tone Tax Payment Limit, the business customer will be notified that they have exceeded their limit, via automatic notification, and that they should contact your financial institution. The tax payment will not be accepted for posting.

Computer Transmission Limit – establishes the maximum amount that will be accepted by your institution in a single computer transmission from your business customer. If the transmission amount exceeds this limit, your business customer will be informed they have exceeded their computer transmission limit, via automatic notification, and that they should contact your financial institution. The computer transmission will not be accepted for posting.

Total Daily Limit – establishes the maximum dollar amount of transactions your financial institution will accept in a single day from a business customer. When determining if the customer is within their total daily limit, the system will combine all credit transactions posted by your business customer for the requested posting date. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on the Daily Risk Report. Upon review of the Daily Risk Report, you may contact your business customer informing them they have exceeded their risk limit.

Risk Management & Best Practices
State & Federal Tax Payments

Establishing Risk Limit Exposures (continued)

Your institution should review the Daily Risk Report prior to transmitting files to the ACH network. In the event it is determined a business customer's transmission should be cancelled, your institution will have the opportunity to remove the transactions from the file.

Example: If you set the Total Credit Limit to $20,000 and your customer transmits a payroll for $12,000, a transfer of funds for $4,000 and a tax payment of $5,000, an Over Daily Limit message will be printed on your Daily Risk Report and show an over limit of $1,000.

48 Hour Limit - establishes the maximum dollar amount your financial institution will accept in a 48-hour timeframe (two banking business days) from your business customer. The system will combine all credit transactions posted by your business customer during the last 48 hours. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit.

10 Day Limit - establishes the maximum dollar amount your financial institution will accept in a ten (10) day period from your customer. The system will combine all credit transactions posted by your business customer during the last ten days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit.

30 Day Limit - establishes the maximum dollar amount your financial institution will accept in a thirty (30) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last thirty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your business customer informing them they have exceeded their risk limit.

Risk Management & Best Practices
State & Federal Tax Payments

Establishing Risk Limit Exposures (continued)

60 Day Limit - establishes the maximum dollar amount your financial institution will accept in a sixty (60) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last sixty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit.

Restricting Transaction Type

Your financial institution may restrict the transaction types your business customer is allowed to use.

If the business customer transmits a transaction type that has not been authorized by your financial institution, the file transmission will be rejected. Your business customer will receive a notification indicating that the transmission has been rejected.

Balanced File

This option allows your financial institution to require your business customers to transmit a balanced file (credit dollar amount is equal to the debit dollar amount). When this option is activated, the system will not allow your business customer to transmit an out of balance file to your financial institution.

If your customer transmits an out of balance file, the transmission will be rejected. Your business customer will receive a notification indicating that the transmission has been rejected.

You should not use this option if your internal banking system is expecting files to be offset by a pre-loaded account number assigned to a specific business customer.

Risk Management & Best Practices
State & Federal Tax Payments

Establishing Risk Limit Exposures (continued)

Offset Account Number

This feature is used in conjunction with the Balanced File option and Batch Authentication option. This feature allows your financial institution to designate the exact corporate account(s) your business customer may debit when transmitting a tax payment batch.

Establishing Delay Days

If your customer is using the IVR (Interactive Voice Response) System to post tax payments, you may want to debit your customer's account two to three days ahead of the scheduled posting date to ensure funds are available.

A Tax Trust Transfer Delay Days option gives your financial institution time to create a debit to your customer's business account and if the debit is returned as non-sufficient, your institution will have time to cancel the payment to the government or contact your customer and collect the funds.

When your financial institution activates the Tax Trust Transfer Delay Days option, the system will automatically create two batches of transactions each time your customer posts a tax payment.

The first batch of transactions will debit your customer's business account the next business day and credit your financial institution's Tax Trust Settlement Account. A second batch is created with the number of delay days your institution has imposed. A standard number of delay days are two (2).

By establishing a two (2) day delay in transmitting payments to the government, your financial institution's risk exposure has been reduced, based on the fact that there is a higher confidence level that collected funds were in the possession of your institution prior to the release of the tax payment to the government.

Risk Management & Best Practices
State & Federal Tax Payments

(This page intentionally left blank

Risk Management & Best Practices
Remote Deposit Capture

Initial Setup

Business customers requesting Remote Deposit Capture (converting paper checks received via mail, in person, or drop box) should complete the following forms prior to starting their Remote Deposit Capture program:

Remote Deposit Service Agreement – the agreement should state the terms, conditions, liabilities, responsibilities, and other items that relate to the responsibilities of your financial institution and your business customers.

ACH Origination Service Agreement – if your financial institution will permit your business customer to convert paper checks into eligible ACH transactions, you should sign an ACH Origination Service Agreement with your business customer.

Credit Authorization – your business customer should provide this form, or similar authorization, which directs your financial institution to deposit an offset credit to the checks processed via the Remote Deposit Capture service to a specific account(s).

Your financial institution may allow deposits to be made to more than one corporate account.

Risk Exposure Assessment

Your financial institution's risk exposure for the Remote Deposit Capture service can be generated from several events and activities including, but not limited to:

Duplication of Checks – a business customer could attempt to scan a check more than once. This includes a check scanned twice in the same day or checks that have been scanned in a previous day's deposit. A business customer could attempt to scan a check that is more than a year old. Therefore, your institution should monitor checks scanned by your customer for a period time to ensure customers are not scanning checks twice.

Risk Management & Best Practices
Remote Deposit Capture

Risk Exposure Assessment (continued)

Duplicate Deposits – a business customer intent on committing fraud could install a Remote Deposit Capture service from multiple financial institutions, allowing the business to scan checks on the same day using multiple service providers.

A business customer could also take the checks that were scanned to a branch office of your institution or deposit the checks at another financial institution.

Change Deposit Account – when your financial institution allows a business customer to scan checks and make deposits to multiple accounts, or your institution does not restrict the deposit account, checks not authorized to be deposited to an account can be misdirected.

Example: a business owner could attempt to deposit a check written to the business into their personal account or an employee can misdirect the company's deposit to their own personal account.

MICR Line Manipulation – allowing a business to alter the MICR line mechanically read from the check can permit the check to be drawn from an unauthorized account.

Amount Manipulation – when your financial institution allows a business customer to enter the amount of the check, the business can alter the check, which could result in an unauthorized transaction.

Excessive Deposits – a business customer intent on committing fraud could process fraudulent checks in one large deposit on a specific day, which could provide the business customer with additional opportunities to receive unauthorized funds.

Conversion of Checks to ACH – should your financial institution determine that the cost benefits are achieved by converting eligible checks to ACH transactions, your financial institution is responsible for verifying the business customer is following all ACH related check conversion rules.

Risk Management & Best Practices
Remote Deposit Capture

Establishing Risk Limit Exposures

The system allows your institution to establish a series of Risk Limit Exposures. By using each of the following limits, liability Risk Exposure can be reduced.

Total Daily Limit – establishes the maximum dollar amount of transactions your financial institution will accept in a single day from a business customer. When determining if the customer is within their total daily limit, the system will combine all credit transactions posted by your business customer for the requested posting date. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on the Daily Risk Report. Upon review of the Daily Risk Report, you may contact your business customer informing them they have exceeded their risk limit. Your business customer may request that their daily limit be increased.

48 Hour Limit - establishes the maximum dollar amount your financial institution will accept in a 48-hour timeframe (two banking business days) from your business customer. The system will combine all credit transactions posted by your business customer during the last 48 hours. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit. Your customer may request that their 48-hour limit be increased.

10 Day Limit - establishes the maximum dollar amount your financial institution will accept in a ten (10) day period from your customer. The system will combine all credit transactions posted by your business customer during the last ten days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit. Your customer may request that their ten (10) day limit be increased.

30 Day Limit - establishes the maximum dollar amount your financial institution will accept in a thirty (30) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last thirty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your business customer informing them they have exceeded their risk limit. Your customer may request that their thirty (30) day limit be increased.

Risk Management & Best Practices
Remote Deposit Capture

Establishing Risk Limit Exposures (Continued)

60 Day Limit - establishes the maximum dollar amount your financial institution will accept in a sixty (60) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last sixty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit. Your customer may request that their sixty (60) day limit be increased.

Restricting Transaction Type

Your financial institution may restrict the transaction types your business customer is allowed to use.

If the business customer transmits a transaction type that has not been authorized by your financial institution, the file transmission will be rejected. Your business customer will receive a notification indicating that the transmission has been rejected.

Example: your financial institution can limit the type of ACH transactions eligible checks can be converted to, i.e. POP, ARC, BOC, and RCK.

Should your financial institution determine converting eligible checks to ACH risks do not outweigh the benefits received; your institution has the option of blocking the conversion of any and all checks to an ACH transaction.

MICR Line Adjustment

This feature will prevent a business customer from altering the MICR line of a check. When a check's MICR line cannot be correctly read, the system will reject the check from the daily deposit.

Prior to activation of the MICR Line Adjustment feature, your financial institution should determine if your business customer poses a significant threat as related to this risk exposure. If so, the business customer will need to deposit checks that are rejected due to MICR line errors at your nearest branch office.

Risk Management & Best Practices
Remote Deposit Capture

Duplicate Check Override

The system will compare each check scanned to the check history database that is stored on your business customer's check processing system. When a duplicate check is located, a warning box is displayed requiring an employee or company manager to enter the Duplicate Check Override Password.

The Duplicate Check Override Password allows the system to accept a check where the routing number, account number, and check numbers are identical.

The Duplicate Check Override Password should not be provided to the company employee designated to scan checks and transmit deposit files.

Duplicate Check Warning Email

The system verifies transmitted checks to a check history database that contains checks processed during the prior six (6) months. When a duplicate check is located, a Duplicate Check Warning email is transmitted to the business customer and the financial institution warning both parties that a duplicate check(s) has been processed.

Because many duplicate check are often legitimate (i.e. starter check kits), the duplicate check warning will not automatically suspend a batch from posting.

Same Day Duplicate Check Email

The system verifies transmitted checks to a check history database that contains checks that have been processed during the current business day. When a same day duplicate check is located, a special email is transmitted to the business customer and the financial institution warning both parties that a same day duplicate check(s) has been transmitted by the business customer.

To reduce risk, the system automatically drops same day duplicate checks from the deposit.

Check Acceptance

At the time checks are scanned any check not in standard check formatting is automatically rejected.

Risk Management & Best Practices
Remote Deposit Capture

Automatic Suspend Batch

This feature allows your financial institution to manage risk by establishing a transaction limit, transmission limit, and daily limit for each business customer. When a business transmits a remote deposit file which exceeds any of the pre-established limits, the batch will be automatically suspended.

The system will send an email to your designated staff alerting them a batch has been suspended and is waiting for their review and release. Your staff can access the image of each check within the batch to verify its accuracy and legitimacy.

The system allows your staff to remove any check within the batch. Should an item be removed, your business customer will receive an email noting the adjustment to their daily deposit.

Risk Management & Best Practices
International ACH Transactions

Overview

International ACH Transactions (IAT) can be used for a variety of business needs, including business customers initiating credits to pay employees in other countries, withdraw payments from foreign trading partners, and collecting international consumer payments.

Financial institutions often use the International ACH Transaction service to transfer funds from an internal consumer or business account to an international account, at the request of the account holder.

The following pages discuss *Best Practices* for each of these business environments.

IAT - Initial Setup

Verify with your business customer that they have obtained a signed copy for each pre-authorized payment and that the company will store the forms in a safe place for a minimum period as outlined in the NACHA rules.

IAT Risk

The following examples reflect risk impact that can be realized and considered by your institution when processing deposit transactions via IAT.

The NACHA rules state that once your institution has sent International transactions to your ACH Operator (typically the Federal Reserve Bank via FedACH or your direct ACH gateway), your financial institution has guaranteed the funds, whether or not you have collected the funds.

Therefore, your institution should have a high confidence rating that on the day the funds are debited from the business customer's corporate account, the fully collected funds will be available.

Customer Does Not Have a Corporate Account at Your Institution – when you allow a business to debit a corporate account located at another financial institution to fund the disbursement of IAT credits, your financial institution may have a higher degree of risk exposure based to the fact that, your institution has guaranteed the funds but you do not have the offset funds in your possession.

Risk Management & Best Practices
International ACH Transactions

IAT Risk (continued)

Funds Deposited by Corporate Check – when your institution accepts a paper corporate check drawn on a foreign financial institution for the offset of IAT credits, your institution may be accepting a higher risk exposure based on the fact that, the RDFI may decline the check.

To mitigate your institution's risk, you should consider establishing a line-of-credit, obtain collateral sufficient to cover disbursed funds while the check clears, or use other methods that would guarantee the availability of funds when the check is presented to the receiving institution.

Funds Deposited by Wire Transfer – when wire transfers are used to offset the disbursed payments, your institution should verify the wire transfer has been completed prior to the release of the payment transactions to the ACH Network.

Funds Deposited by Cashier's Check – Cashier's checks should be validated prior to the release of payments to the ACH Network.

Funds Are Drawn from a Deposit Account Located at Your Institution - this practice provides a lesser degree of risk exposure than funds drawn off a foreign corporate account, but still needs to be evaluated. The primary risk exposures are a) the funds in the offset corporate account are not 'collected' funds, b) the company withdraws the funds between the time your institution releases the deposit payments and the day the offset debit is applied to the corporate account.

To mitigate your institution's risk exposure when processing a consumer bill payment transaction your institution should consider the following:

- Establish an ACH offset corporate account for each business where the offset ACH credits to consumer bill payments are held.

- Delay transferring corporate offset credits to the business customer's corporate account for a given number of days. When determining the number of Funds Transfer Delay Days your institution should consider international transactions can take a much longer time to be returned than ACH transactions that were generated on accounts that are located at a United States financial institution.

Risk Management & Best Practices
International ACH Transactions

IAT Risk (continued)

- Establish a line of credit for the business that is sufficient to cover returned international ACH transactions for any given day.

Place a hold on funds located in the business corporate account equal to the consumer bill payments that are to be disbursed

Establishing IAT Risk Limit Exposures

The system allows your institution to establish a series of Risk Limit Exposures. By using each of the following limits, liability exposure can be reduced.

Per Transaction – this option allows your institution to establish the maximum amount of a single deposit. When activated, the system will automatically reject a file that is transmitted by your business customer if a credit transaction exceeds the set amount.

Per Batch Limit – this option allows your financial institution to establish the maximum batch amount. When activated, the system will automatically reject a file that is transmitted by your business customer if the dollar amount of the batch transmitted exceeds the set limit.

When using the Per Batch Limit option, your institution must define each batch that will be accepted by your financial institution by assigning a specific company ID and batch description to each batch transmitted by your business customer.

Browser Based Transmission Limit – establishes the maximum amount that will be accepted by your institution in a single computer transmission. When the transmitted amount exceeds this limit, your business customer is informed they have exceeded their computer transmission limit, via automatic notification. The computer transmission will not be accepted for posting. The business customer may contact your institution and request their limit be increased.

Total Daily Limit – establishes the maximum dollar amount of transactions your financial institution will accept in a single day from a business customer. When the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on the Daily Risk Report. Upon review of the Daily Risk Report, you may contact your business customer informing them they have exceeded their risk limit. Your business customer may request their daily limit be increased.

Risk Management & Best Practices
International ACH Transactions

Establishing IAT Risk Limit Exposures (continued)

Your institution should review the Daily Risk Report prior to transmitting files to the ACH Network. In the event it is determined a business customer's transmission should be cancelled, your institution will have the opportunity to remove the transactions from the file.

Example: If you set the Total Credit Limit to $20,000 and your customer transmits an IAT payroll for $12,000, a transfer of funds for $4,000 and a tax payment of $5,000, an Over Daily Limit message will be printed on your Daily Risk Report and show an over limit of $1,000.

48 Hour Limit - establishes the maximum dollar amount your financial institution will accept in a 48-hour timeframe (two banking business days) from your business customer. The system will combine all credit transactions posted by your business customer during the last 48 hours. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit. Your customer may request that their 48-hour limit be increased.

10 Day Limit - establishes the maximum dollar amount your financial institution will accept in a ten (10) day period from your customer. The system will combine all credit transactions posted by your business customer during the last ten days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of the Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit. Your customer may request that their ten (10) day limit be increased.

30 Day Limit - establishes the maximum dollar amount your financial institution will accept in a thirty (30) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last thirty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your business customer informing them they have exceeded their risk limit. Your customer may request that their thirty (30) day limit be increased.

Risk Management & Best Practices
International ACH Transactions

Establishing IAT Risk Limit Exposures (continued)

60 Day Limit - establishes the maximum dollar amount your financial institution will accept in a sixty (60) day period from your business customer. The system will combine all credit transactions posted by your business customer during the last sixty days. If the combined dollar amount from all transaction postings exceeds this amount, your business customer will be placed on your Daily Risk Report. Upon review of your Daily Risk Report, you should contact your customer informing them they have exceeded their risk limit. Your customer may request that their sixty (60) day limit be increased.

IAT- Offset Account Number

This feature allows your financial institution to designate the exact corporate account(s) your business customer may debit when transmitting an IAT Batch. Your institution may establish up to three offset account numbers. The system will check each of the Offset Account Number fields for a possible match and will automatically reject the business customer's file transmission if a match is not located.

IAT OFAC Compliance

The NACHA, government, and banking rules stipulate financial institutions must follow OFAC rules and regulations when transmitting and receiving international ACH transactions.

Your financial institution can activate the OFAC Verification option available through the International Payroll Direct Deposit system. When activated, the system will check credit transactions against the published OFAC list provided by the federal government.

When the system locates a match from the name entered on the credit transaction to the names provided on the OFAC Block list, your financial institution is notified via an email notice.

When your financial institution is notified of a possible OFAC transaction match, your institution should review the transaction further to determine if this is an actual name on the list, or if the OFAC match generated a 'false positive.'

Risk Management & Best Practices
International ACH Transactions

IAT OFAC Compliance (continued)

When you have determined a 'false positive' has been generated, your institution can release this transaction and add the specific routing number, account number, and name to an OFAC Approved Transaction list which will allow future transactions to be transmitted by the employer for this deposit account, circumventing future OFAC blocks.

Risk Management & Best Practices
On-Demand Transfers

Purpose

The On-Demand Transfers service provides your institution's account owners the convenience of transferring funds to and from their personal deposit accounts within your institution quickly and safely. Your consumers can also transfer funds out of accounts held at other financial institutions into accounts with your institution, or from your institution to the consumer's accounts held elsewhere.

If desired, your institution can limit transfers to incoming credits only. For an added convenience, your account owners can schedule transfer requests up to 30 days in advance of their requested posting date. The On-Demand Transfers service stores the consumer's transfer, or loan payment, information and posts it on the exact day they select.

Risk Assessment

Your financial institution's Risk Exposure can be increased and decreased as risk variables are added or removed from the Risk Probability equation.

The following examples reflect risk impact that can be realized and considered by your institution when processing On-demand Transfer transactions.

Your financial institution should remember the NACHA rules state that once your institution has transmitted deposit transactions to the ACH operator, typically the Federal Reserve Bank via Fed ACH or your direct ACH gateway, your financial institution has guaranteed the funds.

Consumer Generates a Debit to an Unauthorized/Fraudulent Account – When a consumer debits an unauthorized/fraudulent account at another financial institution, the transfer will be rejected and returned to your institution. This can be a risk exposure to your institution if the Returned Debit transaction is not received prior to your financial institution releasing the offsetting credit to the consumer. If you allow your account holder to withdraw or transfer their On-demand Transfer credit to another institution, you may not have offsetting funds in your possession, and therefore, you would sustain a loss.

Consumer Generates Debit at a Financial Institution but the Account Does Not Exist – When a consumer debits an unauthorized/fraudulent account at another financial institution, the transfer will be rejected and returned to your institution. This can be a risk exposure to your institution if the Returned Debit transaction is not received prior to your financial institution releasing the offsetting credit to the consumer. If you allow your account holder to withdraw or transfer their On-demand Transfer credit to another institution, you may not have offsetting funds in your possession, and therefore, you would sustain a loss.

Risk Management & Best Practices
On-Demand Transfers

Risk Assessment (continued)

Insufficient Funds in Consumer's Account Located at Your Institution – When your account holder has insufficient funds in their account, which is located at your institution, this can create a risk exposure when the consumer deposits their On-Demand Transfer offset credit to another financial institution. If your financial institution releases the credit offset to the ACH network before the debit transaction is verified against the account holder's available funds, your institution may sustain a loss since when your institution transmits the credit offset via the ACH network, your institution has guaranteed the funds.

Insufficient Funds in Consumer's Account Located at Another Financial Institution – When you allow account holders to debit accounts located at another financial institution, and there are insufficient funds, the transfer will be rejected and returned to your institution. This can create a risk of exposure if your institution has allowed your account holder to withdraw funds, thus leaving no asset to collect the returned payment from.

Debit and Credit Accounts Located at Another Institutions in a Single Transfer – when your financial institution allows account holders to transfer funds between accounts, which are both located at other financial institutions, your institution may be exposed to financial losses if the Debit transaction is return as Uncollectable and your account holder has no funds available at your institution to cover the returned debit transaction. This practice has a high degree of risk exposure and should be carefully considered prior to policy implementation.

Risk Controls

Know Your Account Holder – a common fraud technique is to open a new account, use the On-Demand Transfer system to withdrawal funds from an account at another institution, which doesn't exist or have any available funds, and then extract the funds from the credit transaction via in-person, ATM or debit card before your financial institution has received the returned uncollectable debit transaction. Therefore, you should consider restricting your On-Demand Transfer service to specific account holders until they have demonstrated the ability to manage their money such as, carrying a reasonable average balance.

Your account holder should not have a history of writing insufficient checks or late loan payments.

Establish an On-Demand Transfer Standard Policy on Daily Transfer Limits – your financial institution should consider establishing an On-Demand Transfer Daily Transfer Limit which would establish a risk limit that is acceptable to your organization.

Risk Management & Best Practices
On-Demand Transfers

Risk Controls (continued)

Establish an Account Holder Daily Transfer Limit – this feature would allow your financial institution to establish an On-Demand Transfer Daily Transfer Limit which would be best suited for each account holder.

Limit Transfer Credits – your financial institution may consider limiting the amount of credit transactions that deposit to your financial institution. This would prevent account holders from transmitting funds via the ACH network to another institution prior to your validation of available funds to cover the debit.

Note: most institutions do not select this option since it often places the institution at a competitive disadvantage.

Delay Availability of Funds – check with your institution's core processor to see if credit transactions can be included in your available balance calculations. A two (2) day hold on the funds should cover as much as 98% of returned uncollectable debit transactions.

Open a Line of Credit Account- consider establishing a Line of Credit unsecured loan for each member whereby the loan's available credit is always sufficient to cover the Daily On-Demand Transfer Limit. By doing so, when an On-Demand Transfer debit is returned to your institution as Uncollectable, and the account holder has depleted their checking and savings account balance, your institution would have the ability to recover the funds by an advance on the Line of Credit Account.

Note: If the On-Demand Transfer offsetting credit was to a loan account, most financial institutions simply reverse the loan payment as if the account holder had written a bad paper check.

Verify Account Ownership with a Micro Deposit – prior to sending the first credit or debit to another financial institution, consider generating an internal deposit and withdrawal to the account. Limit the amount to be under $3.00, but more than $0.25, and do not use the same micro deposit amount for all account holders.

Transmit the credit first, and at the same time, send an email to your account holder requesting they confirm the deposit amount. This will require your account holder to log into their account, thus confirming ownership, or contact the individual that will be receiving credits in the future.

After your account holder has confirmed the micro deposit amount, inform the account holder that you will be issuing a debit to retrieve your institution's micro deposit confirmation amount. This will test the account to ensure the account holder has not placed electronic debit blocks on their account.

Risk Management & Best Practices
On-Demand Transfers

(This page intentionally left blank)

Risk Management & Best Practices
New Account Funding

Purpose

Allowing new account holders to fund their new account via an ACH debit from an account located at their current financial institution or by using their credit or debit card has become standard practice in the financial industry.

While this has become the funding of choice for more new account holders, your financial institution should consider the risks and implement proper safeguards to protect your institution's assets.

Risk Exposure Assessment

Your financial institution's Risk Exposure can be increased and decreased as risk variables are added or removed from the Risk Probability equation.

The following examples reflect risk impact that can be realized which should be considered by your institution when offering new account funding via an ACH transfer of funds or when accepting payment via credit or debit card.

Consumer Generates a Debit to an Unauthorized/Fraudulent Account – When a consumer debits an unauthorized/fraudulent account at another financial institution, the transfer will be rejected and returned to your institution. This can be a risk exposure to your institution if the Returned Debit transaction is not received prior to your financial institution releasing the offsetting credit from the New Account Funding transaction to the consumer.

If you allow your new account holder to make cash withdrawals or transfer their New Account Funding credit to another institution, you may not have offsetting funds in your possession, and therefore, your financial institution could sustain a loss.

Consumer Generates Debit at a Financial Institution but the Account Does Not Exist – When a consumer debits an unauthorized/fraudulent account at another financial institution, the transfer will be rejected and returned to your institution. This can be a risk exposure to your institution if the Returned Debit transaction is not received prior to your financial institution releasing the offsetting credit to the consumer. If you allow your account holder to withdraw or transfer their New Account Funding credit to another institution, you may not have offsetting funds in your possession, and therefore, you would sustain a loss.

Risk Management & Best Practices
New Account Funding

Risk Assessment (continued)

Insufficient Funds in Consumer's Account Located at Another Financial Institution – When you allow account holders to debit accounts located at another financial institution, and there are insufficient funds, the transfer will be rejected and returned to your institution. This can create a risk of exposure if your institution has allowed your account holder to withdraw New Account Funding credit, thereby leaving no asset to collect the returned payment from.

Credit and Debit Card Chargebacks – When a consumer uses a fraudulent credit or debit card the credit card rules allow the violated party to issue a chargeback to your financial institution. While the ACH rules typically limit unauthorized debit returns to sixty (60) days, the credit card rules extend that timeline up to a year.

Therefore, it is important that your financial institution establish controls for your New Account Funding program that will limit risk exposure

Risk Mitigation (Controls)

Know Your Account Holder – a common fraud technique is to use the New Account Funding option when opening a new account to withdraw funds from an account at another institution or credit card, which doesn't exist or have available funds, and then extract the funds from the credit transaction via in-person, ATM or debit card before your financial institution has received the returned uncollectable debit transaction.

Therefore, you should consider restricting your new account holder from accessing funds until a reasonable period of time has passed, thus providing your institution with a comfort level that a valid debit was issued.

Establish an New Account Opening Policy Limiting Funding Amounts – your financial institution should consider establishing a limit on the amount of funds that you will permit when using your online New Account Opening service via an ACH transfer and credit card cash advance.

Delay Availability of Funds – check with your institution's core processor to see if the New Account Funding credit transaction can be included in your available balance calculations. A four (4) day hold on the funds should cover as much as 98% of returned uncollectable debit transactions.

Risk Management & Best Practices
New Account Funding

Risk Assessment (continued)

Deposit Funds to a GL Account – your financial institution may consider depositing New Account Funding credits that are generated via an ACH debit or credit card cash advance, into a General Ledger account. This will prevent your new account holder from withdrawing funds while your institution is establishing the account and confirming the credit worthiness of your new account holder.

Risk Management & Best Practices
New Account Funding

(This page intentionally left blank)

Risk Management & Best Practices
Multi-Level/Multi Factor Login Authentication

Multi-Level Login Authentication

Multi-Level Authentication procedures are required by the financial institution industry to protect unauthorized access to sensitive information stored on the company's network.

Magic-Wrighter uses multi-level authentication as its default. Your financial institution's and business customer's initial login authentication procedures will require the following steps:

1. Enter assigned username.
2. Establish individual security ID, including selecting a picture and describing the picture.
3. Select three (3) security questions and provide answers to questions. These answers will be used in the future when additional login verification is required.
4. Use temporary password provided by authorized account representative.
5. User is required to change temporary password to continue login process.

The multi-level login will allow the system to track all users accessing the administration portal and, if necessary, determine if additional security information is required during the login process.

When additional information is required, security questions are presented. The user will be required to provide the answer entered at the time of initial login and account setup.

To increase file authentication security, business customers should have separation of duties, where employee one prepares the file for transmission, employee two, or manager, logs in and transmits file and manager two uses the file authorization IVR system.

Multi-Factor Login Authentication

Multi-factor login includes requirements of multi-level login authentication procedures. However, multi-factor does not permanently store the user's password. With multi-factor, when the user logs into the system, Magic-Wrighter generates a one-time password with a two (2) minute time-to-live. The user may opt to receive an email or use a mobile app that generates the matching one-time password.

Utilizing multi-factor procedures makes the login process more secure than multi-level login authentication. When using the multi-factor login authentication procedure, your financial institution's and business customer's initial login will require the following steps:

Note: The user must request random password generation via email or must download an approved random generator app at time of user account setup.

Risk Management & Best Practices
Multi-Level/Multi Factor Login Authentication

Multi-Factor Login Authentication

1. Enter assigned username
2. Establish individual security ID, including selecting a picture and describing the picture.
3. Select three (3) security questions and provide answers to questions. These answers will be used in the future when additional login verification is required.
4. Use one-time password received via email or mobile app within the required period of time.

All financial institution employees and managers should use multi-factor login procedures. In addition, financial institutions should require business customers, with higher degree risk exposure use multi-factor login procedures.

Risk Management & Best Practices
Multi-Level File Posting Authentication

Multi-Level File Transmission Posting Authentication

After the data center's secure transaction server has accepted the business customer's transaction file via the Internet download option, it will provide the customer with a file received acknowledgement. This acknowledgement is displayed on the customer's screen.

After the business customer has successfully downloaded authorized transactions, the transmitted file must be authenticated using the interactive voice response file (IVR) authorization system or Internet.

Dual file posting control has been provided to the business customer to mitigate the risk of processing unauthorized transactions.

Proper use of the multi-level dual authorization requires one business customer employee to download a transaction file via the Internet and a second employee to authenticate the file, which will release the file for posting.

The employee with operator rights to download the file will be issued their own Internet access codes, passwords, and multi-level login security codes to transmit ACH files to the secure transaction server.

A second employee will be issued an IVR or Internet user access code and password, which are required for authenticating transmitted files to the data center.

The IVR authentication process requires the authenticating employee to enter the total file credits and debits transmitted to the data center. These two amounts are verified to the actual ACH file that was received by the data center's secure transaction server.

If the amounts do not match, the transmitted ACH file is automatically rejected and removed from the system.

After each authentication, the authenticating operator will receive a file transmission confirmation via fax and/or email. The file transmission fax phone number and/or email address is established at the time the business customer is added to the data center's secure database and can only be changed by request from the business customer or financial institution in writing.

Risk Management & Best Practices
Multi-Level File Posting Authentication

(This page intentionally left blank)

Risk Management & Best Practices
Browser Based ACH Direct

Browser Based System Overview

When your business customer uses the browser-based system for ACH transaction processing, all data is stored on a secure network. All confidential banking information is stored using a 256 AES or higher encryption.

Business customers should use the authentication option that best suits their environment. Your financial institution should educate and encourage your business customers to use the highest possible level of file authentication to minimize their company's risk exposure.

The browser-based system contains features that provide your financial institution more control over ACH transactions that are processed by your business customers, thereby allowing your institution to mitigate risk exposures by applying additional controls.

Initial Setup

Business customers requesting employee payroll direct deposit should complete the following forms prior to starting their direct deposit program:

Payroll Direct Deposit Debit Authorization – provides your financial institution with authorization to withdraw funds from the business customer's corporate account to offset the credits due each employee.

Your financial institution must follow the NACHA rules and store this authorization for the complete time service is provided and a minimum of two years after termination of the authorization or service.

Note: This form may not be required if your financial institution allows your business customer to transmit a balanced file where the total credits and total debits within the file are equal.

Payroll Processing – provides your institution with the description of the payroll, frequency to expect the payroll, and contact information. This information will allow your ACH department to establish a payroll transmission calendar. The calendar can be used to monitor expected employer payroll transmissions, allowing you to red flag unauthorized transmissions.

Risk Management & Best Practices
Browser Based ACH Direct

Initial Setup (continued)

Employee Payroll Direct Deposit Authorization – NACHA requires all originators, in this case your business customer, to obtain permission to deposit payments into an employee's checking or savings account. Your institution should verify your business customer is using an authorization form that follows the NACHA authorization guidelines.

Verify with your business customer that they have obtained a signed copy from each employee requesting payroll direct deposit and that the company will store the forms in a safe place for a minimum period as outlined by NACHA rules.

Risk Exposure Assessment

Your financial institution's risk exposure can be increased and decreased as risk variables are added or removed from the risk probability equation.

The following examples reflect risk impact that can be realized and considered by your institution when processing employee direct deposit transactions.

The NACHA rules state that once your institution has sent employee payroll direct deposit transactions to the ACH Operator (typically the Federal Reserve Bank via FedACH or your direct ACH gateway), your financial institution has guaranteed the funds.

The NACHA rules also permit employee payroll direct deposit transactions to be transmitted by your institution to the ACH Network up to two (2) days in advance of the posting due date, but only allows your institution to transmit the offset payroll debit one day in advance.

Your institution should have a high confidence rating that on the day the funds are debited from the business customer's corporate account, the fully collected funds will be available.

Customer Does Not Have a Corporate Account at Your Institution – when you allow a business to debit a corporate account located at another financial institution to cover the disbursement of funds, your financial institution will experience a higher degree of risk exposure, due to the fact that if payment is not received prior to the release of the deposits, your institution has guaranteed the funds to the ACH Network and you do not have offset funds in your possession.

Risk Management & Best Practices
Browser Based ACH Direct

Funds Deposited by Corporate Check – when your institution accepts a paper corporate check to offset the disbursed payments, your institution is accepting uncollected funds. This means that if there are insufficient funds in the corporate account or the account has been closed at the time the check clears, the RDFI will return the check, creating a risk exposure.

Funds Deposited by Wire Transfer – when wire transfers are used to offset the disbursed payments, your institution should verify the wire transfer has been completed prior to the release of the payment transactions to the ACH Network.

Funds Deposited by Cashier's Check – Cashier's checks should be validated prior to the release of payments to the ACH Network.

Funds Are Drawn from a Deposit Account Located at Your Institution - this practice provides less risk exposure than funds drawn from a foreign corporate account, but still needs consideration. The primary risk exposures are a) the funds in the offset corporate account are not collected funds, b) the company withdraws the funds between the time your institution releases the deposit payments and the day the offset debit is applied to the corporate account.

Offset Account

To mitigate your institution's risk exposure when releasing credit transactions to the ACH Network, your institution should consider the following:

- Establishing an ACH offset corporate account for each business where funds are deposited and offset funds for disbursed ACH credits are held.
- Prior to the release of ACH credit transactions to the ACH Network, verify collected funds are in the ACH offset corporate account.
- Establish a line of credit for the business sufficient to cover disbursed ACH credits on any given day.
- Place a hold on funds located in the business corporate account equal to the credits that are to be disbursed.

Risk Management & Best Practices
Browser Based ACH Direct

Establishing Risk Limit Exposures

The system allows your institution to establish a series of risk limit exposures. By using each of the following limits, liability exposure can be reduced.

Per Transaction – this option allows your institution to establish the maximum amount of a single Transaction acceptable by your financial institution. The system will automatically block and notify your business customer when the transaction exceeds the set amount.

Per Batch Limit – this option allows your financial institution to establish the maximum batch amount. The system will automatically block and notify your business customer if a batch total exceeds the established amount.

Total Daily Limit – establishes the maximum transaction dollar amount for a single posting day from a business customer. The system will combine all like transactions credit/debits posted by your business customer for the requested posting date. If the combined amount from all transactions submitted for a given posting date exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their daily limit be increased.

48 Hour Limit - establishes the maximum dollar amount your financial institution will accept in a 48-hour timeframe. The system will combine all like- transactions, credits/debits, posted by your business customer during the last two (2) banking business days. If the combined amount submitted during the given time exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their 48-hour limit be increased.

10 Day Limit - establishes the maximum amount your financial institution will accept in a ten (10) calendar day period from your customer. The system will combine all like transactions credit/debits posted by your business customer during the last ten (10) days. If the combined amount from all transactions exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their ten (10) day limit be increased.

Risk Management & Best Practices
Browser Based ACH Direct

Establishing Risk Limit Exposures (continued)

30 Day Limit - establishes the maximum amount your financial institution will accept in a thirty (30) calendar day period from your business customer. The system will combine all like transactions credit/debits posted by your business customer. If the combined amount exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their thirty (30) day limit be increased.

60 Day Limit - establishes the maximum amount your financial institution will accept in a sixty (60) calendar day period from your business customer. The system will combine all like transactions credit/debits posted by your business customer during the last sixty days. If the combined amount exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their sixty (60) day limit be increased.

Restricting Transaction Type

Your financial institution may restrict the transaction types your business customer is allowed to use. The business customer would be unable to initiate a transaction type your financial institution has not previously approved for their use.

Balanced File

This option allows your financial institution to require that your business customers transmit a balanced file (credit and debit dollar amounts are equal). When this option is activated, the system will not allow your business customer to transmit an out of balance file to your financial institution.

If your customer transmits an out of balance file, the transmission will be rejected and will be notified that the transmission has been rejected.

You should not use this option if your internal banking system is expecting files to be offset by a pre-loaded account number assigned to a specific business customer.

Risk Management & Best Practices
Browser Based ACH Direct

Offset Account Number

This feature is used in conjunction with the balanced file option. This feature allows your financial institution to designate the exact corporate account(s) your business customer may debit when transmitting a payroll direct deposit batch. Your institution may establish up to three offset account numbers. The system will check each of the offset account number fields for a possible match and will automatically reject the business customer's file transmission if a match is not located.

File Posting Email

When authentication is required to complete the release of a batch, an email confirmation will be sent to the authenticator's email address. The email is your business customer's verification that the released batch has been accepted by the system. To reduce the company's risk exposure, the email address should not be that of the employee who entered or authenticated and released the transactions for posting.

Your financial institution continues to mitigate risk by including multiple parties in the file posting and release process.

Batch Posting Authentication

Your financial institution may establish a batch posting authentication requirement for your business customers to follow.

The batch posting authentication feature is designed to reduce the risk exposure to your business customer from an unauthorized transfer of funds to or from your business customer's corporate account. The feature will also reduce risk exposure to your financial institution by requiring more than one business customer employee to validate file posting.

In the event your financial institution does not require batch posting authentication, your business customer can still establish the requirement when they initially create a batch. Your business customer may determine that their company will benefit from this feature by reducing their risk exposure, based on the fact they can require the authorization of two employees to release and post this batch

Risk Management & Best Practices
Browser Based ACH Direct

Internet Batch Posting Authentication

Batch posting authentication can be performed via the Internet. To mitigate risk exposure, the business customer employee assigned to perform batch posting authentication will be assigned a personal login username, password, security key, and will be required to use the multi-level login procedures to release the transactions within each batch.

Telephone Internet Batch Posting Authentication

Batch posting authentication can be performed via the interactive voice response (IVR) system. To mitigate risk exposure, the business customer employee assigned to batch posting authentication will be required to dial into a toll free 800 number and authenticate each file posting by entering their assigned personal login access code, password, and the authentication number assigned to the posted file.

Fax or Email Confirmation

Your business customer will receive a fax and/or email confirmation after the posting file has been accepted. To mitigate risk exposure, your business customer should request the confirmation be delivered to an employee other than the employee(s) who posted and/or authenticated the file. Your business customer is responsible for reviewing the confirmation.

The confirmation will verify the amount of the transmission and the posting date. The confirmation will also verify that the file was received and accepted for processing.

If it is not accepted, the confirmation will indicate the file was rejected and the reason why it was not accepted.

Your business customer should keep the confirmation for proof of file posting.

Risk Management & Best Practices
Browser Based ACH Direct

(This page intentionally left blank)

Risk Management & Best Practices
Browser Based Remote Deposit Capture

Browser Based System Overview

When your business customer uses the browser-based system for remote deposit capture, all data is stored on a secure network. All confidential banking information is stored using a 256 AES or higher encryption.

Business customers should use the authentication option that best suits their environment. Your financial institution should educate and encourage your business customers to use the highest possible level of file authentication to minimize their company's risk exposure.

The browser-based system contains features that provide your financial institution more control over remote deposit capture transactions that are processed by your business customers, thereby allowing your institution to mitigate risk exposures by applying additional controls.

Initial Setup

Business customers requesting to convert paper checks that were received via mail, in person, or drop box should complete the following forms prior to starting their remote deposit capture program:

Remote Deposit Service Agreement – the agreement should state the terms, conditions, liabilities, responsibilities, and other items that relate to the responsibilities of your financial institution and your business customers.

ACH Origination Service Agreement – if your financial institution will permit your business customer to convert paper checks into eligible ACH transactions, you should sign an ACH Origination Service Agreement with your business customer.

Credit Authorization – your business customer should provide this form, or similar authorization, which directs your financial institution to deposit an offset credit to the checks processed via the Remote Deposit Capture service to a specific account(s).

Your financial institution may allow deposits to be made to more than one corporate account.

Risk Management & Best Practices
Browser Based Remote Deposit Capture

Risk Exposure Assessment

Your financial institution's risk exposure for the remote deposit capture service can be generated from several events and activities including, but not limited to:

Duplication of Checks – a business customer could attempt to scan a check more than once. This includes a check scanned twice in the same day or checks that had been scanned in a previous day's deposit. A business customer could attempt to scan a check that is more than a year old.

Duplicate Deposits – a business customer intent on committing fraud could install a remote deposit capture service from multiple financial institutions, allowing the business to scan checks on the same day using multiple service providers.

A business customer could also take the checks that were scanned to a branch office of your institution or deposit the checks at another financial institution.

Change Deposit Account – when your financial institution allows a business customer to scan checks and make deposits to multiple accounts or your institution does not restrict the deposit account, checks not authorized to be deposited to an account can be misdirected.

> Example: a business owner could attempt to deposit a check written to the business into their personal account or an employee can misdirect the company's deposit to their own personal account.

MICR Line Manipulation – allowing a business to alter the MICR line mechanically read from the check can permit the check to be drawn from an unauthorized account.

Amount Manipulation – when your financial institution allows a business customer to enter the amount of the check, they can alter the check, which could result in an unauthorized transaction.

Excessive Deposits – a business customer intent on committing fraud could process fraudulent checks in one large deposit on a specific day, which could provide the business customer with additional opportunities to receive unauthorized funds.

Conversion of Checks to ACH – should your financial institution determine that the cost benefits are achieved by converting eligible checks to ACH transactions, your financial institution is responsible for verifying the business customer is following all ACH related check conversion rules.

Risk Management & Best Practices
Browser Based Remote Deposit Capture

Offset Account

To reduce your institution's risk exposure when releasing credit transactions to the ACH network, your institution should consider the following:

- Establishing an ACH offset corporate account for each business where funds are deposited and offset funds for disbursed ACH credits are held.
- Prior to the release of ACH credit transactions to the ACH network, verify collected funds are in the ACH offset corporate account.
- Establish a line of credit for the business sufficient to cover disbursed ACH credits on any given day.
- Place a hold on funds located in the business corporate account equal to the credits that are to be disbursed.

Establishing Risk Limit Controls

The system allows your institution to establish a series of risk limit exposures. By using each of the following limits, liability exposure can be reduced.

Per Transaction – this option allows your institution to establish the maximum amount of a single transaction that has been approved by your financial institution. The system will not allow your business customer to submit a batch containing items that exceeds the pre-established limit.

Per Batch Limit – this option allows your financial institution to establish the maximum batch amount. The system automatically blocks and notifies your business customer if a batch total exceeds the pre-established limit.

Total Daily Limit – establishes the maximum transaction dollar amount your financial institution will accept for a single posting day from a business customer. The system combines all like transactions credits/debits posted by your business customer for a specified date. If the combined amount from all transactions submitted for a given posting date exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them that they have exceeded their limit is displayed and they are prompted to contact your institution should they wish to request that their daily limit be increased.

Risk Management & Best Practices
Browser Based Remote Deposit Capture

Establishing Risk Limit Controls (continued)

48 Hour Limit - establishes the maximum amount your financial institution will accept in a 48-hour timeframe (two banking business days) from your business customer. The system combines all like transactions credit/debit posted by your business customer during the last 48 hours. If the amount from all transactions submitted during the given time exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their 48-hour limit be increased.

10 Day Limit - establishes the maximum dollar amount your financial institution will accept in a ten (10) day period from your customer. The system will combine all like transactions credit/debit posted by your business customer during the last ten days. If the combined amount from all transactions submitted during the given time exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their ten (10) day limit be increased.

30 Day Limit - establishes the maximum amount your financial institution will accept in a thirty (30) day period from your business customer. The system will combine all like credit/debit transactions posted by your business customer during the last thirty days. If the combined dollar amount from all transactions submitted during the given time exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their thirty (30) day limit be increased.

60 Day Limit - establishes the maximum amount your financial institution will accept in a sixty (60) day period from your business customer. The system will combine all like credit/debit transactions posted by your business customer during the last sixty days. If the combined dollar amount from all transactions submitted during the given time exceeds the pre-established limit, your business customer will be blocked from submitting the batch. A screen notifying them they will exceed their limit is displayed and they are prompted to contact your institution should they wish to request their sixty (60) day limit be increased.

Risk Management & Best Practices
Browser Based Remote Deposit Capture

Offset Account Number

This feature allows your financial institution to designate the corporate account(s) the processed checks will be deposited to

Restricted Access

The system allows your business customer to establish access to the electronic payment service for multiple employees within their company as they deem necessary. The restricted access feature can restrict a specific batch from being viewed and changed by other authorized employees who have access to the Browser Based system.

Example: One employee may have access to the Browser Based Remote Deposit Capture service, but not a batch where corporate funds are transferred.

Batch Posting Authentication

Your financial institution may establish a batch posting authentication requirement. This feature will force your business customer to use the batch posting authentication procedure.

The batch posting authentication feature is designed to reduce the risk to your business customer from an unauthorized processing of checks by requiring more than one business customer employee to validate file posting.

In the event your financial institution does not require batch posting authentication, your business customer can still establish the requirement when they initially create a batch. Your business customer may determine that their company will benefit from this feature by reducing their risk exposure, based on the fact they can require the authorization of two employees to release and post this batch.

Batch Posting Authentication

Batch posting authentication can be performed via the Internet. The business customer employee assigned to perform batch posting authentication will be assigned a personal login username, password, security key to release the transactions within each batch.

Risk Management & Best Practices
Browser Based Remote Deposit Capture

Fax or Email Confirmation

Your business customer will receive an email confirmation after the posting file has been accepted. To provide dual control of batch postings your business customer should request the confirmation to be delivered to an employee other than the employee(s) who posted and/or authenticated the file. Your business customer is responsible for reviewing the confirmation.

The confirmation will confirm the amount of the transmission and the posting date. The confirmation will also verify that the file was received and accepted for processing.

If the file is not accepted, the confirmation will indicate the file was rejected and the reason why it was not accepted.

Your business customer should keep the confirmation for proof of file posting.

Risk Management & Best Practices
eCommerce Services

Overview

When your financial institution uses Magic-Wrighter's Web hosted eCommerce services, you must ensure that only authorized payments are processed and that limits are in place to reduce fraud exposure.

Customer Identification

To ensure legitimate individuals are using the eCommerce services, a billing file containing the customer's billing account number, name, amount due, due date and a secondary identification (i.e., telephone number, street addressing, etc.) should be downloaded to the eCommerce system. This should occur each billing cycle, weekly, or daily to ensure current data is available for identification of new users during the eCommerce registration process.

Establishing Risk Limit Exposure

The system allows your institution to establish a series of risk limit exposures. By using each of the following limits, liability exposure can be reduced.

Per Transaction – this option allows your institution to establish the maximum amount of a single payment acceptable by your financial institution. The system will automatically block and notify your business customer when the transaction exceeds the set amount.

Total Daily Limit – establishes the maximum dollar amount of transactions for a single posting day from a business customer. The system will combine all like transactions credit/debits posted by your business customer for the requested posting date.

Unlike some business customer products, the system will not automatically block daily eCommerce from processing. This is due to real-time acceptance of eCommerce payments. Therefore, to properly manage business customers using eCommerce services financial institutions should activate the Suspended Batch option. Once set, when daily file amounts exceed the "Total Daily Limit" the business customer's eCommerce batch will be suspended allowing your institution time to review and approve activity.

Risk Management & Best Practices
eCommerce Services

Web Debit Rule

When accepting eCommerce Web debit payments where funds are withdrawn from another financial institution, Originators must use a commercially reasonable account validation method. This validation process may include any of the following:

- Consumer provides copy of current bank account statement.
- A micro deposit is generated requiring customer verification of deposit amount.
- Certified third-party account verification.

Chargebacks and Returned Payments

eCommerce is now the preferred method hackers utilize to commit fraud. Therefore, your institution should monitor business customers returned ACH payments and credit card chargebacks closely to protect against excessive fraud activity.

When your financial institution is using MWI eCommerce services for internal payments such as loans, new account opening, A2A, or other services, ensure staff fully understand MasterCard, Visa, and NACHA ecommerce rules and regulations.

Credit Card Self-Assessment

All institutions and business customers accepting eCommerce credit card payments are required to complete an annual self-assessment and provide a report copy to MWI. To learn more about PCI self-assessment requirements visit www.visa.com.

Risk Management & Best Practices
Account Data Compromise

Account Data Compromise

Magic-Wrighter takes precautions to protect the privacy of its users. If at any time you believe personal information not authorized by a user of the Magic-Wrighter payment services was disclosed to any individual or entity, please contact a Magic-Wrighter representative immediately.

Make a written record of all information that was provided to you or of your personal observations.

MasterCard Site Data Protection Program

In addition to meeting PCI Data Security Standards each merchant or sub merchant (school) is required to comply with the MasterCard Site Data Protection program, which is designed to ensure credit and debit card data is protected against compromise.

Risk Management & Best Practices
Account Data Compromise

(This page intentionally left blank)

Risk Management & Best Practices
Business Customers

Management should ensure only authorized personnel have access to confidential banking and transaction data. It is important that your financial institution's management create *Best Practices* that incorporate all risk aspects of safeguarding company and customer confidential data. The following *Best Practices* should be incorporated with additional security standards that best fit your organization's needs.

- **Isolated Workstation –** an isolated workstation should be installed to access reports and files, perform transmissions and customer maintenance, and other services provided to your organization.

  The workstation should be installed with a read only CD or hard drive. The system should install a fresh operating system each time the workstation is powered up. A good operating system for this environment is Linux; however, other operating systems will also allow this feature.

  No USB ports should be allowed to store any data.

  The workstation should be powered off when each operator has completed their immediate task. When not in use, the workstation should be powered off.

- **Email Access –** no email access should be permitted on the isolated workstation.

- **Non-Isolated Workstation** – when it is not practical to have an isolated workstation available to access sensitive banking transaction information, your staff should be educated to spot suspicious emails purporting to be from any financial institution, government department or agency, or other sources requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN, pass phrases, and similar information.

  Avoid opening file attachments or clicking on web links in suspicious emails. By doing so, you can infect your workstation and network with malicious code.

- **Web Access –** your IT department should take steps to initiate web filtering, prohibiting access to any web site that is not directly related to the services that are being provided to you or that are considered banking and payment related web sites which are specifically required to perform your organization's confidential data access needs.

Risk Management & Best Practices
Business Customers

- **File Attachments** – employees should be trained not to open an email file attachment from unknown sources. Many email attachments appear to be pictures but have been altered to infect your workstation and network with malicious code.

- **Firewall –** your IT department should install a firewall to prevent unauthorized access to your workstation and network. The firewall should be configured by an experienced firewall expert and reviewed at least annually or after changes to your network have been performed.

  Firewall operating software should be kept up to date according to the vendor's recommendations.

- **Usernames –** each employee requiring access to confidential data should be provided a unique username. Employees should be instructed never to share their username or other login information with another employee or anyone outside your company.

- **Strong Passwords** – employees should be provided a temporary password during their initial set up. The employee should be required to change their temporary password at their initial access to the system. Employees should be required to change their passwords at least quarterly, but not less than semi-annually.

  Employees should be instructed to enter a minimum of fifteen (15) characters when creating their password. The password should contain upper- and lower-case letters, numbers, and special characters. Employees should not use consecutive numbers or letters within their password and should avoid using children's names, names of pets, home address, phone numbers and other information that could be easily guessed.

- **Sharing Login Information** – employees should never share their usernames or passwords with other employees or anyone outside your company. Employees should be advised not to store their passwords on their personal computers or printed copies in their desk where easily accessible.

- **Avoiding Dual Usage** – employees should avoid using the same password when logging in to different web sites. If compromised on a less protected web site, hackers can obtain faster access to more well protected web sites when employees use the same password.

Risk Management & Best Practices
Business Customers

- **Third Parties** – never share your login user names or passwords with a third-party requiring access to your workstation or system. Third parties should be provided temporary login user names and passwords or cleared for permanent access to the system. Careful consideration should be given when determining whether to provide third parties with login information. Third Parties should be required to demonstrate they have a full understanding of your policies requiring access and safeguarding of confidential data.

- **Administration Rights** – employee workstations and system access should not be allowed by accessing the systems via administrator login control. Employees should be provided with restricted user rights and only allowed access to the minimum data required to perform their duties. User rights must not permit the download and deployment of executable code.

- **Anti-Virus Software** – commercial grade anti-virus software should be installed on all workstations and servers connected to your internal network. Updates of anti-virus definitions and vendor software should be applied when required.

- **Operating System** – it is important that all workstations, servers, and appliances connected to your network have vendor patches applied according to vendor recommendations. When possible, patches should be applied first to test equipment to ensure new patches do not adversely affect your network.

- **Spyware** – the installation of commercial grade spyware detection software can protect your network from malicious spyware code.

- **Browser Caching** – employees should clear their browser cache before starting a new session to clear copies of web pages that have been stored from their last session. This is easily accomplished by selecting new session, or a similar option, depending on the browser installed on your workstation.

- **Use Secure Websites** – when accessing a website where confidential data will be exchanged, verify that a secure session has been activated. The letters 'https' (not just 'http') should be displayed in your web browser's URL line. You should also see a security symbol displayed, such as a padlock.

- **Auto Login** – employees should not use automatic login options that save user names or passwords.

- **Session Time-Outs** – secure web sites should contain automatic timeouts when not in use, requiring the employee to log back into the system. If the website does not have an automatic timeout, employees should be instructed to log out when not in use. Employees should never leave their workstation while logged in to secure websites.

Risk Management & Best Practices
Business Customers

- **Foreign Terminal Usage** – employees should never use a workstation at a public library, hotel, coffeehouse, or internet cafe to access confidential information. In no case should an employee use wireless access at home, while traveling, or any other wireless access that is not directly connected to your company's network.

- **User Obligations** – it is important that your institution educates users of the electronic payments services you provide to consumers and business customers in conjunction with our services utilized by your financial institution. Users should understand their obligation to follow security protocol.

- **Alert Centers** – subscribe to websites, news outlets, security vendors, and other third parties that will automatically notify you when data breaches, new viruses, fraud alerts, and other issues are identified that could impact your financial institution or customer.

- **Act Immediately** – should you discover any suspicious transactions or activity with your account, contact our customer relations department immediately. Your institution or business customer has limited time to act regarding fraudulent transactions.

- **Phishing Education –** you should provide training to staff authorized to access confidential data. Employees should be trained not to respond to emails requesting their password, user name, or any information that is already known by the serving vendor.

  Employees should be trained not to reply to an email requesting company data, bank information, or any other confidential data, no matter how authentic the email appears.

Risk Management & Best Practices
Sample Forms

The following pages provide sample forms that may assist your institution in following *Best Practices*.

Some forms are intended to act as internal controls to ensure all policies and procedures have been followed, while other forms are designed to meet NACHA authorization requirements.

Your financial institution may modify these forms to fulfill specific requirements pertaining to product offerings from your institution.

Note: These forms have been developed to work in conjunction with the products and services provided in the Magic-Wrighter suite of electronic payment services.

.

New Customer Checklist

Required Y/N	Completed Initials	
_____	_____	Company Agreement
_____	_____	Company Information Sheet
_____	_____	Fee Schedule
_____	_____	Processing Calendar
_____	_____	Establish Risk Limits
_____	_____	Review Authorization Agreement for Pre-Authorized Deposits
_____	_____	Review Authorization Agreement for Preauthorized Payments
_____	_____	Review ARC/BOC/POP Notice(s)
_____	_____	Review RCK Notice(s)
_____	_____	Review Web Site Security for WEB Payments
_____	_____	Review Authorization Procedures for TEL Payments
_____	_____	Send Required Information to Processing Center
_____	_____	Provide User Manual
_____	_____	Provide NACHA Rules
_____	_____	Schedule Customer Training

Business Name: _____

Contact Name: _____

Phone Number: _____ Fax Number: _____

Risk Limit
Authorization Form

Company Name _____

Type of Business _____ Tax ID # _____

Customer Contact _____ Title _____

Telephone (_____) _____ Fax (_____) _____

Limit Approval Contact _____ Title _____

Telephone (_____) _____ Fax (_____) _____

Process Risk Limits for this company? (Y/N) ____

INDIVIDUIAL'S TRANSACTION LIMIT

_____ Per Payroll Cr. Limit
_____ Per Payroll Dr. Limit
_____ Per Transfer/Tax Payment Cr. Limit
_____ Per Transfer/Tax Payment Dr. Limit

_____ 72 Hour Total Cr. Limit
_____ 72 Hour Total Dr. Limit

_____ 10 Day Total Cr. Limit
_____ 10 Day Total Dr. Limit

_____ 30 Day Total Cr. Limit
_____ 30 Day Total Dr. Limit

_____ 60 Day Total Cr. Limit
_____ 60 Day Total Dr. Limit

DAILY LIMITS

_____ Per Batch Cr. Limit
_____ Per Batch Dr. Limit
_____ Total Cr. Limit
_____ Total Dr. Limit

Authorized by:

_____ _____
Print name Signature

Payroll Direct Deposit
Offset Debit Authorization

Company Information:

Name _____

Tax ID Number _____

I (we) hereby authorize _____, hereinafter called FINANCIAL INSTITUTION, to initiate debit entries to my (our) Checking account indicated below.

I (we) understand that our approved transmission limit (risk) is _____ and we must obtain written notification from the FINANCIAL INSTITUTION if/when our transmission amount exceeds this pre-approved amount.

FINANCIAL INSTITUTION:

NAME _____ BRANCH _____

CITY _____ STATE _____ ZIP _____

TRANSIT/ABA NO. _____ ACCOUNT NO. _____

This authority is to remain in full force and effect until FINANCIAL INSTITUTION has received written notification from me (us) of its termination in such time and in such manner as to afford the FINANCIAL INSITUTION a reasonable opportunity to act on it.

NAME(S) _____ TITLE _____
(PLEASE PRINT)

NAME(S) _____ TITLE _____
(PLEASE PRINT)

DATE _____ SIGNATURE _____

Payroll Processing Information

Business Customer Name _____

Contact at Business _____

Contact Phone Number _____

Contact Email Address _____

Description of Payroll _____

Next Payroll Posting Date _____ (Date payroll is to be deposited to employee's account)

Frequency of Payroll ___Weekly ____ Bi-Weekly ____ Semi-Monthly ____ Monthly

Browser Based Service
Authorization Form

Company _____

Address _____

City, State Zip _____, _____ _____

Tax ID _____

Primary Contact Person _____

Contact Day Phone (_____) _____-_____ Fax (_____)_____-_____

E-Mail Address _____

Alternate Contact Person_____

Contact Day Phone (_____) _____-_____ Fax (_____)_____-_____

E-Mail Address _____

Approved Transaction Codes
PPD for employee entries & CCD for corporate offset

Processing Account #_____ Routing #_____

Daily Limit _____ 30 Day Limit _____

Per Batch Limit_____ Per Transaction Limit _____

Financial Institution:

Contact Name _____

Contact Phone (_____) _____-_____ Fax (_____)_____-_____

E-Mail Address _____

Signature _____ **Date** _____

Electronic Payment Authorization

Business Name _____

Business Tax ID # _____

I (we) hereby authorize _____, hereinafter called FINANCIAL INSTITUTION, to initiate credit entries and if necessary debit adjustments to my (our) Checking account indicated below

Financial Institution Name _____
Routing Number _____

Account Number _____

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

Name(s) _____ ID Number _____
(Please Print) (SS#)

Date _____ Signature _____

Pre-Authorized Payment Agreement

Business Name _____

Business Tax ID # _____

I (we) hereby authorize _____, hereinafter called BUSINESS, to initiate debit entries to my (our) Checking account indicated below, located at the financial institution name listed below, hereinafter called FINANCIAL INSTITUTION and to debit the same to such account shown below.

Financial Institution Name _____

City _____ State ____ Zip _____

Routing Number _____

Account Number _____

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

Name(s) _____ ID Number _____
(Please Print) (SS#)

Date _____ Signature _____

Risk Management & Best Practices
Business Customer Best Practices

The following examples illustrate the computations that are made by the system to arrive at risk limit overages.

Condition #1

Customer has a $100,000 daily limit
Customer is only scheduled for a 12:00 PM run
The Thursday noon run has been processed
Next scheduled run is Friday 01/18 where transaction will be pulled date up to 01/22
Customer transmits the following batches at 3:00PM
This transmission would be accepted

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21 Holiday	Tuesday 01/22

$40,000 PD 01/17 Transmitted Batch
$40,000 PD 01/18 Transmitted Batch
Total Risk at this transmission time is $80,000.00

Condition #2

Customer has a $100,000 daily limit
Customer is only scheduled for a 12:00 PM run
The Thursday noon run has been processed
Next scheduled run is Friday 01/18 where transaction will be pulled date up to 01/22
The customer transmitted a file at 10:00 AM on Thursday morning for $40,000 that was accepted and processed PD for 01/18
Customer transmits the following batches at 3:00PM
This transmission would be rejected

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21 Holiday	Tuesday 01/22

$40,000 PD 01/18 Transmitted Batch
$40,000 PD 01/19 Transmitted Batch
$40,000 PD 01/22 Transmitted Batch
Total Risk at this transmission time is $120,000.00

Risk Management & Best Practices
Business Customer Best Practices

Condition #3

Customer has a $100,000 daily limit
Customer is only scheduled for a 12:00 PM run
The Thursday noon run has been processed
Next scheduled run is Friday 01/18 where transaction will be pulled date up to 01/22
The customer transmitted a file at 10:00 AM on Thursday morning for $40,000 that was accepted and processed PD for 01/18
Customer transmits the following batches at 3:00PM
This transmission would be accepted

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21
Tuesday 01/22	Wednesday 01/23			
				Holiday

$40,000 PD 01/17 Transmitted Batch
$40,000 PD 01/18 Transmitted Batch
$40,000 PD 01/23 Transmitted Batch
Total Risk at transmission time is $80,000.00

Condition #4

Customer has a $100,000 daily limit
Customer is scheduled for a 12:00 PM run and the 4:00 PM run
The Thursday noon run has been processed but not the 4:00 PM run
Next scheduled run is Thursday 01/18 a 4:00 PM where transaction will be pulled date up to 01/22
The customer had transmitted $60,000 with a PD of 01/17 Thursday morning and the batch was processed during the Thursday noon run
Customer transmits the following batches at 3:00PM
This transmission would be accepted

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21
Tuesday 01/22	Wednesday 01/23			
				Holiday

$30,000 PD 01/18 Transmitted Batch
$60,000 PD 01/17 Processed at Noon sitting in History
Total Risk at transmission time is $90,000.00

Risk Management & Best Practices
Business Customer Best Practices

Condition #5

Customer has a $100,000 daily limit
Customer is scheduled for a 12:00 PM run and the 4:00 PM run
The Thursday noon run has been processed but not the 4:00 PM run
Next scheduled run is Thursday 01/18 at 4:00 PM where transaction will be pulled date up to 01/22
The customer had transmitted $60,000 with a PD of 01/17 Thursday morning and the batch was processed during the Thursday noon run
Customer transmits the following batches at 3:00PM
This transmission would be rejected

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21
Tuesday 01/22	Wednesday 01/23			
				Holiday

$30,000 PD 01/18 Transmitted Batch
$30,000 PD 01/12 Transmitted Batch
$60,000 PD 01/17 Processed at Noon sitting in History
Total Risk at transmission time is $120,000.00

Condition #6

Customer has a $100,000 daily limit
Customer is scheduled for a 12:00 PM run and the 4:00 PM run
The Thursday noon run has been processed but not the 4:00 PM run
Next scheduled run is Friday 01/18 at 4:00 PM where transaction will be pulled date up to 01/22
The customer had transmitted $60,000 with a PD of 01/18 Friday morning and the batch was processed during the Thursday noon run
Customer transmits the following batches at 3:00PM
This transmission would be accepted

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21
Tuesday 01/22	Wednesday 01/23			
				Holiday

$30,000 PD 01/18 Transmitted Batch
$30,000 PB 01/23 Transmitted Batch
$60,000 PD 01/17 Processed at Noon sitting in History
Total Risk at transmission time is $90,000.00

Risk Management & Best Practices
Business Customer Best Practices

Condition #7

Customer has a $100,000 daily limit
Customer is scheduled for a 12:00 PM run and the 4:00 PM run
The Friday noon run has been processed but not the 4:00 PM run
Next scheduled run is Friday 01/18 at 4:00 PM where transaction will be pulled date up to 01/22
Customer transmits the following batches at 3:00PM
This transmission would be accepted

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21 Holiday
Tuesday 01/22	Wednesday 01/23			
Thursday 01/24	Friday 01/25	Saturday 01/26	Sunday 01/27	Monday 01/28
Tuesday 01/28				

$30,000 PD 01/18 Transmitted Batch
$30,000 PB 01/28 Transmitted Batch
$60,000 PD 01/18 Processed at Noon sitting in History
Total Risk at transmission time is $90,000.00

Condition #8

Customer has a $100,000 daily limit and today is 01/18/2013
Customer is scheduled for a 12:00 PM run and the 4:00 PM run
The Friday noon run has been processed but not the 4:00 PM run
Next scheduled run is Friday 01/18 at 4:00 PM where transaction will be pulled date up to 01/22
The customer transmitted on 01-15 a batch for $40,000 dated 01/25 and on 01-16 customer transmitted a $30,000 batch dated 01/28
Customer transmits the following batches at 3:00PM on 01/18
This transmission would be rejected

Thursday 01/17	Friday 01/18	Saturday 01/19	Sunday 01/20	Monday 01/21 Holiday
Tuesday 01/22	Wednesday 01/23			
Thursday 01/24	Friday 01/25	Saturday 01/26	Sunday 01/27	Monday 01/28
Tuesday 01/29				

$40,000 PD 01/25 Previously Transmitted Batch still unprocessed
$30,000 PB 01/28 Previously Transmitted Batch still unprocessed
$40,000 PD 01/26 Transmitted Batch
Total Risk at transmission time is $110,000.00

Risk Management & Best Practices
Restrict FI Staff via IP Address

Financial institution staff requiring access to the FI Administration Portal (ELB) may be restricted to a specific IP address or a range of IP addresses. This practice will prohibit staff from using computers and personal devices from outside the financial institution's network to access customers and consumer confidential banking information.

To activate the restriction to specific IP addresses, contact a CSR

Risk Management & Best Practices
Business Customer Best Practices

Change Control:

September 27, 2021 – Add MasterCard Site Data Protection Program
October 22, 2021 – Annual Review; update logo and grammatical changes
November 16, 2021 - Add eCommerce best practices (section 15)
September 16, 2022 – Removed Child Support Sample Form (EOL)
September 16, 2022 – Annual Review – no recommended changes
November 2, 2022 – Add Restrict FI Staff via IP Address
October 27, 2023 – Annual review; update formatting (AC, BOD)