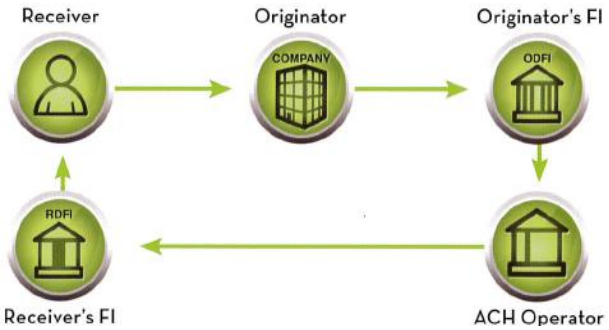
ARMSTRONG BANK

CORPORATE USER
ACH QUICK REFERENCE CARD

ACH BASICS

What is the ACH Network?

The Automated Clearing House (ACH) Network is a network created for the electronic movement of money and other related data. This is a safe, secure, and reliable network for direct consumer, business, and government payments. As the migration from paper to electronic payment continues, the cost-effective ACH Network grows and enables innovation that strengthens the industry with creative payment solutions.



Who are the ACH Participants?

There are five key participants that contribute to the successful completion of an ACH transaction:

- The **Receiver** can be either an individual or a company that has authorized the Originator (you) to credit or debit their account. Examples might be employees receiving a payroll deposit or customers receiving a withdrawal for payment of goods or services.
- The **Originator** is the entity that has been authorized by the Receiver to either credit or debit their account. If you are sending the employee's payroll deposit or customer's payment, your company is the Originator.
- The **Originating Depository Financial Institution (ODFI)** is the financial institution with which your company has the contractual relationship for ACH Services.
- The **ACH Operator** is the central clearing facility for ACH transactions.
- The **Receiving Depository Financial Institution (RDFI)** is a financial institution with which the Receiver has an account relationship.

As an Originator, what are the responsibilities?

In creating and sending transactions through the ACH Network, you have a few responsibilities as part of your agreement with us. One piece of the agreement states that you agree to abide by the Rules and Guidelines established by NACHA as well as making sure that the transactions are legal. Simply stated, when you send a transaction you are guaranteeing (warranting) that:

- The transactions are authorized by the Receiver
- The transactions are correct and comply with the Rules
- The information used for transaction creation is secure at all times

All other requirements are based off of those warranties.

What are the Authorization requirements?

NACHA states that transactions sent through the ACH Network (with the exception of person to person payments) must be authorized. Along with this, companies sending ACH transactions must be able to prove that the transactions that they send are authorized. Listed below are the types of transactions that you may be able to do and their requirements.

Transaction Type	Authorization Requirements	Retention Requirements
Consumer Credits (PPD). Consumer credits are widely known as Direct Deposits or Direct Deposits via ACH. This can be used to send funds to a consumer defined as a live person for a number of reasons including payroll, reimbursement, disbursements, etc.	The Originator (you) must have authorization, either oral or written from the consumer (Receiver) prior to initiating the credit entry.	While the Rules do not require the Originator to retain the Direct Deposit authorization, if there is a written copy, it is in your best interest to do so for two years beyond the life of the payments.
Consumer Debits (PPD). Consumer debits, known as Direct Payments, are used to collect funds from consumer accounts. This could be single or recurring payments for bills, dues, contributions, payments, etc.	Originating companies must have a written authorization from the consumer (Receiver) to initiate a PPD debit entry. Additionally, the authorization must provide the consumer with a method to revoke authorization, and a copy of the authorization must be provided to the consumer.	The consumer's authorization for a PPD debit entry must be retained for two years beyond the life of the payments. Upon written request, a copy of the authorization must be provided to the RDFI within 10 banking days of the request.

Authorization Requirements (cont.)

Transaction Type	Authorization Requirements	Retention Requirements
Consumer Payments by Telephone (TEL). These payments are either initiated by the consumer or by the Originator only if there is an existing relationship. You must verify the customer using commercially reasonable procedures before completing the transaction.	For single entry transactions, Originators must maintain audio recordings of the oral authorization or provide a written notice to the Receiver. For recurring entries, Originators must do both, maintain audio recordings and provide a written notification.	For single entries, the original or a copy of the audio recording or a copy of the written notification must be retained for two years from the authorization. For recurring entries, the original or a copy of the audio recording and a copy of the written notification must be retained for two years from the termination or revocation of the authorization.
Consumer Payments by Internet (WEB). These are payments which are made by a website. You must provide a way to verify the customer using commercially reasonable procedures before completing the transaction.	A written authorization is obtained via the Internet or wireless network either for single entry or recurring entries.	The authorization must be retained for two years from the date of the authorization on a single entry and for two years from the termination or revocation of the authorization for recurring entries.
Corporate Credits or Debits (CCD). These are transactions to move funds from company to company.	The Originator must obtain an authorization but there is no rule dictating the form of the authorization. A written authorization is implied.	It is in the best interest that any written authorizations be kept for two years from the termination of the authorization. If requested by RDFI, the Originator must be able to provide the written record or, at minimum, your business name and a phone number or email address for authorization inquiries.

What is a Prenotification (Prenote)?

One of the ways that you can help make sure that the transactions are correct is by sending Prenotifications before sending your first transaction. Prenotifications (prenotes) are zero dollar entries used by your company to verify that the account number on an entry is for a valid account at an RDFI. Prenotes are optional and can be sent with an ACH application. If your company chooses to send prenotes, you are required to do so at least 3 banking days before sending the first live dollar entry.

If there are any errors in a prenote entry or it cannot be processed, a Notification of Change (NOC) or return will be sent by the RDFI to notify your company of the necessary corrections to be made.

What is a Notification of Change (NOC)?

As mentioned, the RDFI will send a Notification of Change (NOC) if something needs to change within the transaction. This is a non-monetary entry which allows the RDFI to return information to the ODFI and Originator without returning the value of the entry. Some of the reasons an NOC might be sent would be an incorrect account number, incorrectly coded as checking or savings, a bank merger with a new routing and account number, or a once valid routing number needs to be changed. With these types of transactions, the RDFI is stating that the information that they are providing is correct and is therefore liable if the information is incorrect. Upon receipt of an NOC, your ODFI must report NOC information to you. You are required to make the changes noted in the NOC before that transaction is sent again or within 6 banking days, whichever is later. The change codes used in the ACH Network and their descriptions are as follows:

Change Codes Used by RDFI	Description of Error	Action Required by Originator
C01	**Account Number** – The account number is incorrect.	Change the Receiver's account number record so the correct information is entered.
C02	**Routing Number** – A previously valid routing number is no longer valid and must be changed.	Change the Receiver's financial institution routing number so the correct information is entered.

ARMSTRONG BANK

CORPORATE USER
ACH QUICK REFERENCE CARD

NOTIFICATION OF CHANGE

Notification of Change Codes (cont.)

Change Codes Used by RDFI	Description of Error	Action Required by Originator
C03	**Routing Number and Account Number** – The routing number and account number are incorrect.	Change the Receiver's financial institution routing number and account number so the correct information is entered.
C04	**Account Name** - The customer has changed the name on the account or the Originator has submitted the name incorrectly.	Change the Receiver's individual name or receiving company name so the correct information is entered.
C05	**Transaction Code –** An incorrect transaction code is causing the entry to be routed to the wrong type of account.	Change the type of account. The account type is indicated on the ODFI's report by a two-digit transaction code. Contact your ODFI if clarification is needed.
C06	**Account Number and Transaction Code** – The account number is incorrect and the transaction is being routed to the wrong type of account.	Change the Receiver's financial institution routing number, account number, and type of account so the correct information is entered.
C07	**Routing Number, Account Number and Transaction Code** – The routing number, account number and account type are incorrect.	Change the Receiver's financial institution routing number, account number, and type of account so the correct information is entered.
C09	**Individual ID Number –** Individual ID Number is incorrect.	Change the individual ID Number so the correct information is entered.
C13	**Addenda Format Error** – The Entry Detail Record was correct, but the information in the Addenda Record was unclear or formatted incorrectly.	Review the formatting in the Addenda Record that accompanied the original ACH entry to determine errors and make corrections using only ANSI standards or NACHA-endorsed banking conventions.

What are Transaction Codes and Why Do They Matter?

ACH entries may be directed to a variety of account types. The Transaction Code describes the type of the payment and the type of Receiving account. If an entry contains an incorrect Transaction Code, the RDFI can send either an NOC or a Return Entry which could describe the error and may provide the correct Transaction Code.

Demand (Checking) Credits		Savings Credits		Financial Institution General Ledger Credits	
Code	Description	Code	Description	Code	Description
21	Notification of Change or Return	31	Notification of Change or Return	41	Notification of Change or Return
22	Deposit	32	Deposit	42	Deposit
23	Prenotification	33	Prenotification	43	Prenotification
24	Zero dollar with remittance data	34	Zero dollar with remittance data	44	Zero dollar with remittance data
Demand (Checking) Debits		**Savings Debits**		**Financial Institution General Ledger Credits**	
Code	Description	Code	Description	Code	Description
26	Notification of Change or Return	36	Notification of Change or Return	46	Notification of Change or Return
27	Payment	37	Payment	47	Payment
28	Prenotification	38	Prenotification	48	Prenotification
29	Zero dollar with remittance data	39	Zero dollar with remittance data	49	Zero dollar with remittance data

ARMSTRONG BANK

CORPORATE USER
ACH QUICK REFERENCE CARD

ACH RETURNS

What is an ACH Return?

An ACH return is an ACH entry that the RDFI is unable to post for reasons defined by the return codes listed in the table below. An RDFI may use the return process for valued ACH entries as well as prenotifications (zero-dollar entries). Most ACH returns must returned to the ODFI within 2 banking days following the Settlement Date of the original entry, with a few exceptions. The ODFI will send notification to you for ALL return entries with a code that describes the reason for the return. The most common codes are listed below with the appropriate action that should be taken for each ACH return.

Reason for Return	Return Code	SEC Code	Return Timeframe	Action by Originator
Insufficient Funds – Available balance not sufficient to cover amount of debit entry.	R01	ALL	2 Banking Days	Originator may initiate a new ACH entry; must be initiated within 180 days of original entry. May not be reinitiated more than two times after original entry.
Account Closed – Previously active account has been closed.	R02	ALL	2 Banking Days	Stop initiation of entries. Contact customer to obtain authorization for another account.
No Account – Account number structure is valid, but doesn't match individual or open account.	R03	All	2 Banking Days	Stop initiation of entries. Customer should be contacted for correct account information.
Invalid Account - Account number structure not valid. Most commonly seen with checking tran codes on savings accounts and vise versa.	R04	All	2 Banking Days	Stop initiation of entries until account number/structure is corrected.
Unauthorized Debit to Consumer Account Using a Corporate SEC Code – A debit entry that uses a corporate SEC code was transmitted to a consumer account but was not authorized by the consumer.	R05	CCD, CTX	60 Calendar Days	Stop initiation of entries.
Authorization Revoked – Customer who previously authorized an entry claims authorization has been revoked from the Originator	R07	PPD, TEL, WEB	60 Calendar Days	Stop initiation of entries until new customer authorization is obtained. Depending on the terms of the original authorization, the Originator may have recourse for collection outside the ACH Network.
Payment Stopped – The customer has requested the stop payment of a specific ACH debit entry.	R08	All	2 Banking Days	Contact the customer to identify the reason for the stop payment and obtain authorization before reinitiating the entry.
Uncollected Funds – Sufficient ledger balance exists, but value of uncollected items brings available balance below amount of debit entry.	R09	All	2 Banking Days	Originator may initiate a new ACH entry; must be initiated within 180 days of original entry. May not be reinitiated more than two times after original entry.
Customer Advises Not Authorized, Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receivers Account– Receiver states the identity of Originator is not known, has no relationship with the Originator, or has not authorized the Originator to debit their account.	R10	All except CCD, CTX	60 Calendar Days	Stop initiation of entries.
Customer Advises Entry Not in Accordance with the Terms of the Authorization - wrong amount; debit date before authorized; incomplete transaction; or improper source document.	R11	All except CCD, CTX	60 Calendar Days	Stop initiation of entries until new customer authorization is obtained. Depending on the terms of the original authorization, the Originator may have recourse for collection outside the ACH Network.

ACH Return Reasons (cont.)

Reason for Return	Return Code	SEC Code	Return Timeframe	Action by Originator
Account Sold to Another DFI – Entry contains routing number for an account that was sold to another financial institution.	R12	All	2 Banking Days	Stop initiation of entries until routing number is corrected.
Invalid ACH Routing Number - Entry contains a Routing Number that is not a valid ACH Routing Number	R13	CCD, CTX	Next file delivery time following processing	Stop initiation of entries until routing number is corrected.
Representative Payee Deceased or Unable to Continue in that Capacity –The representative payee is either deceased or unable to continue in that capacity. The beneficiary is not deceased.	R14	All	2 Banking Days	Stop initiation of entries. Contact customer to obtain authorization for another account.
Beneficiary or Account Holder Deceased – The beneficiary is deceased or the account holder is deceased.	R15	All	2 Banking Days	Stop initiation of entries.
Account Frozen/Entry Returned per OFAC Instructions –Funds unavailable due to specific action taken by the RDFI or by legal action or OFAC has instructed to return the entry.	R16	All	2 Banking Days	Stop initiation of entries.
File Record Edit Criteria or Entry with Invalid Account Number Initiated Under Questionable Circumstances –Common Usage: The Entry contains an invalid account number and is believed by the RDFI to have been initiated under questionable circumstances.	R17	All	2 Banking Days	Stop initiation of entries.
Non-Transaction Account -ACH Entry to a non-Transaction Account or an account that does not accept ACH transactions	R20	All	2 Banking Days	Stop initiation of entries. Contact the customer to obtain authorization for another account.
Credit Entry Refused by Receiver -Any credit entry that is refused by the Receiver may be returned by the RDFI.	R23	All	2 Banking Days following the request from account holder	Stop initiation of entries. Contact the customer to obtain authorization for another account.
Addenda Error –Addenda Record Indicator or Addenda Type Code are incorrect.	R25	All	Next file delivery time following processing	Stop initiation of entries until addenda information is verified. Contact bank if questions with file.
Routing Number Check Digit Error –The ninth digit of the routing number is incorrect	R28	All	Next file delivery time following processing	Stop initiation of entries until routing number is verified. Contact bank if questions with file.
Corporate Customer Advises Not Authorized – Corporate customer has notified that a specific entry is not authorized.	R29	CCD, CTX	2 Banking Days	Stop initiation of entries until subsequent authorization has been obtained. If a valid authorization exists, the Originator may have recourse outside the ACH Network.

ARMSTRONG BANK

CORPORATE USER ACH QUICK REFERENCE CARD

SECURITY POLICY

What about Security?

It is your responsibility to ensure that the information used to make transactions is secure at all times. In 2013, NACHA became more specific with security in passing the Security Framework rules. These rules are designed to ensure that Protected Information (non-public personal information that you used to create an entry or is included in an entry) remains secure from time that it is received until it is destroyed. This includes times when the information is not being used. These rules also require that you, as an Originator, have, enforce, and update security policies or procedures to keep this information safe. These rules also allow the Bank to audit you to verify that you have done the first part, and that you should be willing and able to prove that you have done so.

Policies and Procedures Considerations
What kind of protected information is collected in order to process an ACH entry? Example: Name, SSN, Routing and Account Number
How is that information stored and who has access to it? Employees, Bank, Third-Parties
In the event of a break-in or property destruction, how secure is the information?
How easily could an unauthorized employee have access to protected information?
How is it transmitted? Does a third party (example: payroll or accounting firm) have access to it?
Is the information securely transmitted between you and the third party? Unencrypted Email is not considered a secure method.
If the transactions are uploaded to the Armstrong Bank Cash Management, what happens to the original file? Is it deleted or kept? Is it kept securely?
Once an ACH batch is initiated, is it deleted from Cash Management? If so, after what timeframe? The Bank recommends that you delete previously initiated batches.
What devices are used to access the protected information? Example: Desktop, Laptop, Mobile Device, Saved on CD or USB Drive, etc.
What devices are used to log into Online Banking/Cash Management?
How are these devices secured? Anti-virus, Anti-malware, Passwords, File Deletion software, Encryption software, etc.
What other internet activities are conducted on these devices? Gaming, shopping, email, social media, etc.
Are passwords shared?
What do you do if information becomes compromised?
When you destroy information, how do you destroy it?

In building your security policies and procedures, we also recommend that you include these best practices.

Bank Recommended Best Practices
Use a strong password that is unique to each user and do not share the password with other employees.
Have passwords on your computers and change them regularly.
Have Anti-virus/Anti-malware software and have it regularly scan the computer.
Using business computers for business purposes only.
Make sure that access to protected information is restricted to only necessary personnel.
Educate employees to keep protected information safe and secure at all times including in phone calls, emails, and snail mails.
Educate staff to only click on links from known sources in email, social media, and internet surfing.
Have a Disaster Recovery Plan. FEMA has collected a number of resources to help you do so at http://www.fema.gov/small-business-tools-resources.

For additional resources, please visit **https://www.armstrongbank.com/electronic-banking/annual-education** or contact the Armstrong Bank Treasury Operations Department at 888-221-2265 or treasuryoperations@armstrongbank.com.