	A	B	C	E
3	**ACH GENERAL**			
4	**INTRODUCTION AND PURPOSE**			
5	**ABBREVIATIONS AND DEFINITIONS**			
6	**NCUA REFERENCES**			
7	**EXTERNAL REFERENCES**			
8		**General**	**Yes/No/NA**	**Comments**
9	1.0.0	Is the credit union a Receiving Depository Financial Institution (RDFI)? (Note: Examiners should complete the RDFI questionnaire for credit unions which are RDFIs and limited activity ODFIs to assess the risk associated with the operation.)		
10	1.1.0	Is the credit union an Originating Depository Financial Institution (ODFI) which limits its origination activity to return items only? If yes, go to question 1.4.0.		
11	1.2.0	Does the credit union originate member debit or credit items such as member loan payments or member to member transfers?		
12	1.3.0	Does the credit union permit member business accounts to originate credit items such as payroll for its member business accounts or high risk transactions such as Telephone or Web Initiated Entry (TEL or WEB)?		
13	1.4.0	Does the credit union receive and process its own ACH transactions? If not, provide the name of the third party processor in the comment section, if applicable.		
14	1.5.0	Does the credit union have approved policies and written procedures addressing their ACH operations?		
15	1.6.0	Are the ACH Policies sufficient to address the risks associated with the types and level of risk associated with the credit union's ACH activities? If no or unsure answer the following questions:		
16	1.6.1	Do the policies identify the type of ACH activities initiated at the credit union?		
17	1.6.2	Do the policies provide limitations on transaction amounts and file sizes?		
18	1.6.3	Do the policies ensure adequate segregation of duties (i.e. person creating the file cannot also transmit the file)?		
19	1.7.0	Does the credit union's strategic plan address ACH activities for new initiatives?		
20	1.8.0	Does the credit union have a written organizational chart of the ACH Department?		
21	1.9.0	Does the credit union maintain a Dispute Resolution Log to ensure all issues are resolved in accordance with Reg E requirements? (See Reg E Questionnaire for further discussion on these requirements).		
22	1.10.0	Are employees performing the required checks of ACH items against OFAC SDN Listings?		
23		**Human Resources**	**Yes/No/NA**	**Comments**

	A	B	C	E
3	**ACH GENERAL**			
24	2.0.0	Does the credit union perform checks to determine if the prospective or current employee(s) have been prohibited from being employed at a federally-insured financial institution? If the employee is not prohibited has the credit union performed other types of background checks such as bondability, criminal, and credit on employees with access to the ACH operations?		
25	2.1.0	Is more than one employee involved in the ACH function? If yes, indicate in comment box how many.		
26	2.2.0	Are employees required to take at least 5 consecutive days of vacation and is another employee required to complete the ACH duties?		
27	2.3.0	Does the credit union require ACH personnel to be periodically rotated without prior notice?		
28	2.4.0	Is the credit union a member of the regional payments associations (SWACHA, EastPay, GACHA, MACHA, NEACH, WesPay, UMACHA, etc)?		
29	2.5.0	Are employees performing ACH functions NACHA Certified (AAP- Accredited ACH Professional)?		
30	2.6.0	Are non-AAP certified ACH employees experienced and do they receive training at least annually?		
31	2.7.0	Does the credit union have a nepotism policy restricting related-parties from working in ACH, audit, accounting, and data processing at the same time to eliminate conflicts of interest?		
32	2.8.0	Does the credit union policy require removing permissions and authorities for employees no longer having ACH responsibilities (i.e., to address reassignments, resignations, terminations, etc.)?		
33		**Audit**	**Yes/No/NA**	**Comments**
34	3.0.0	Is an ACH Audit (Independent or Self Audit) completed by a qualified individual, independent of the ACH process, at least annually by December 1 as required by NACHA Rules?		
35	3.1.0	Does internal or external audit staff periodically assess compliance with ACH rules, operating procedures, internal controls, and personnel procedures of the ACH department?		
36	3.2.0	Are findings or areas identified for improvement in audit reports resolved in a timely manner?		
37	3.3.0	Does audit staff keep abreast of planned changes in equipment, systems, and operating procedures to ensure the audit scope is adequate? How do they keep abreast?		
38	3.4.0	Were all concerns about ACH operations in the last regulatory examination report resolved in a timely manner? If NO, please provide comments on the status of the issues identified.		
39	3.5.0	Were all concerns about ACH activities identified in the last annual Supervisory Committee audit resolved in a timely manner? If NO, please provide comments on the status of the issues?		

	A	B	C	E
3	**ACH GENERAL**			
40	3.6.0	Does internal audit staff, if any, receive periodic ACH training including the BSA risk associated with ACH functions?		
41		**Business Continuity Planning**	**Yes/No/NA**	**Comments**
42	4.0.0	Does the credit union's business continuity plan include strategies for restoring ACH operations?		
43	4.1.0	Does the plan include strategies for failure of hardware, software, and communication (communication could include contact with the ACH operator, corporate credit union, members, branches, or data centers)?		
44	4.2.0	Are the strategies and recovery periods reasonable for the size, complexity, and volume of activity of the credit union?		
45	4.3.0	Does the credit union test the BCP plan at least annually?		
46	4.4.0	Are test plans and results documented and adjustments to plans made based on results of the tests in a timely manner?		
47	4.5.0	Is the frequency and methods of testing ACH adequate for the size and complexity of the credit union?		
48	4.6.0	Does ACH personnel receive training at least annually so they understand their responsibilities to restore and/or recover ACH operations?		
49	4.7.0	Are ACH data files, programs, and software backed up on a daily basis, a copy maintained at an off site storage facility, and retained for a period of six years?		
50	4.8.0	Do the recovery files include retention of all entries, including return and adjustment entries, transmitted to and received from the ACH operator?		
51	4.9.0	Are the recovery files periodically tested to determine, at least, the ability to restore the information, the accuracy of the information contained on the file, and the use-ability of the data on the recovery file?		

Cell: A4
Comment: The General ACH Tab is designed to assist examiners to determine the level of review necessary given the types of ACH activities in which the credit union is involved. Questions on this tab will provide an assessment of whether the RDFI, ODFI-Moderate, or ODFI-High Tab should be completed. This tab also covers issues related to Human Resources and Training.

The ACH Network is a batch processing, store-and-forward system. Transactions received by the credit union during the day are stored and processed later in a batch mode. Rather than sending each payment separately, ACH transactions are accumulated and sorted by destination for transmission during a predetermined time period. This provides significant economies of scale. It also provides faster processing than paper checks, which must be physically handled. Instead of using paper to carry necessary transaction information, ACH transactions are transmitted electronically between financial institutions through data transmission.

The ACH Network supports a variety of payment applications. Each ACH application is identified and recognized by a specific three-digit code, know as a Standard Entry Class Code (SEC Code) which appears in the ACH record format. The TEL (Telephone Initiated Entry) is used for the origination of a single entry debit transaction to a member's account pursuant to an oral authorization obtained from a member via the telephone.

Cell: A5
Comment: Abbreviations and Definitions:

ACH - Automated Clearing House
ACH Credits – an ACH transaction which an originator initiates to move funds to a Receiver's account.
ACH Operator - The central clearing facility operated by EPN, a private organization, or the Federal Reserve Bank.
MICR (Magnetic Ink Carriage Return Line) - Magnetically encode line on the bottom of a check.
NACHA - National Automated Clearing House Association
NOC (Notification of Change) - Notification to a merchant from a customer's financial institution indicating the bank account information provided with a specific transaction is incorrect.
OFAC - Office of Foreign Asset Control
Originator – The entity that arranges with an RDFI for ACH entries to be entered into the payment system. An originator may be a company or a consumer.
Originating Depository Financial Institution (ODFI) - A participating financial institution that originates ACH entries at the request of and by agreement with its customers.
PPD (Pre-arranged payment and deposit entry) - The alphabetic mnemonic used to identify credit or debit entries initiated by an originator pursuant to a standing or single-entry authorization from its customer or employee.
Receiving Depository Financial Institution (RDFI) - A financial institution that provides depository account services to consumers, employees, and businesses and accepts electronic debits and credits to and from those accounts. Any financial institution qualified to receive ACH entries that agrees to abide by the NACHA Operating Rules and Guidelines.
Receiver - The person or corporate entity that has authorized a merchant to initiate a refund or charge transaction to their bank account.
Receiving Point - A site where entries are received from an ACH Operator for processing. It may be the RDFI, its data center or a data processing service bureau authorized to receive entries on behalf of a RDFI. Corporate credit unions act as a receiving point on behalf of natural person credit unions.
Sending Point - A processing site from which entries are transmitted to the ACH operator. If may be the ODFI on its own behalf or a financial institution or private data processing service bureau on behalf of the ODFI. Corporate credit unions act, in some instances, as sending points for natural person credit unions.

Cell: A6
Comment: Letter to CU 170-05-95 Automated Clearinghouse - Deposits for Processing Activities

Cell: A7

Comment: (1) NACHA Rules

(2) Treasury Department's Green Book - Rules governing Federal Government payments and reclamations.

(3) FFIEC's Bank Secrecy Act/Anti-Money Laundering Act Examination Guide

(4) 12 CFR Part 205 - Regulation E - Federal Regulation governing consumer electronic transfers/payments.

(5) Title 31 CFR Part 210 - Rules governing Federal Government payments.

(6) FRB Operating Circular 4 and its sub circulars/appendices- Federal Reserve operating circular governing the clearing and settlement of commercial ACH credit and debit items.

(7) 26 CFR Parts 1, 20, 25, 31, and 40 - Federal Regulation governing electronic funds transfers of Federal deposits.

Cell: B9

Comment: ACH activities occur at most credit unions. Smaller credit unions generally are only considered RDFIs. However, all credit unions originate their own returns and are considered an ODFI with limited activity.

Cell: B11

Comment: Loan payments - The member authorizes the credit union to debit their account at another institution and credit their loan at the credit union.

Member to Member transfer - The member authorizes the credit union to debit (or credit) their account at another institution and credit (or debit) their checking or savings account with the credit union. This is similar to a wire transfer but is less expensive than a wire transfer.

Cell: B13

Comment: Many credit unions use correspondent banks or their Corporate Credit Union to facilitate their ACH activities. Examiners should evaluate the controls surrounding these activities by reviewing the agreements between the third party and the credit union. The agreement or procedures should contain limitation on transaction limitations and file size limitation. In addition, procedures should provide for segregation of duties. The employee or operator creating the file should not be the same individual who releases the file into the ACH network. Policies should clearly define activity limitations and proper segregation of duties.

Cell: B14

Comment: Best Practice - A credit union should have an ACH policy and written operating procedure addressing ACH operations. NACHA does not require a written policy and procedure manual, but sound business practices would dictate written guidance. The policy should outline the framework for ACH operations as well as define the level of ACH processing risk the credit union's Board of Directors is willing to accept. The written procedures should document the operational procedures required by management and employees.

Cell: B15

Comment: A well defined ACH policy will include the following components:

(1) The regulatory framework governing ACH operations

(2) The types of ACH activities (ODFI versus RDFI) the credit union will engage in as well as the specific transaction types.

(3) Define the credit union's RDFI responsibilities, and if applicable, ODFI responsibilities.

(4) The level of acceptable risk and risk mitigation factor (system of internal controls)

(5) Define requirements for ongoing training, oversight, audit, records retention, and BCP. and

(6) Ensure compliance with applicable consumer protection and other Federal laws

Cell: B16

Comment: Credit union policies should identify whether they are receiving or originating. If originating, the policies should tell what types of transactions (i.e. loan payments, bill payments, account to account transfers, payroll accounts, donations, or pre-arranged debits, etc.).

Cell: B17

Comment: Management should have set limitations on transaction size and file size based on their level of ACH activity, types of ACH activity, as well as the credit union's size and complexity.

Cell: B18
Comment: This may not be possible in smaller credit unions. Therefore the Board of Directors should approve the policy indicating they are aware and accept the risk associated with the lack of segregation of duties. In addition, the Supervisory Committee should review a random sample of ACH transactions as part of their annual audit.

Cell: B19
Comment: ACH software and related supporting systems can be costly. Additionally, regulatory compliance for various ACH transaction types can be cumbersome. The inclusion of ACH initiatives in the Strategic Plan demonstrates management understands the importance and risk associated with ACH operations.

Cell: B20
Comment: Evidence of a written organizational chart for ACH operations demonstrates management's understanding and importance of segregation of duties. It also allows the examiner to quickly assess appropriate segregation of duties and potential control weaknesses.

Cell: B24
Comment: Credit unions should consult with their attorney or legal staff to ensure they are following various legal requirement before conducting background checks or pulling credit reports. Credit unions need to ensure they are complying with various federal and state statutes.

Cell: B25
Comment: ACH operations should require dual controls and segregation of duties. At a minimum, two employees should be involved in processing activity.

Cell: B28
Comment: Membership in a regional payment association is not required, but these association provide operational resources and training to members. The lack of participation could be an indicator of inadequate training of staff or planning by management.

Cell: B29
Comment: AAP certification is not required but could be an indicator of the level of knowledge and experience employees have of ACH operational and compliance issues.

Cell: B30
Comment: This could be an indicator of employees ability to ensure the credit union is adhering to basic NACHA rules. Periodic training should result in credit union employees keeping current with NACHA rule changes.

Cell: B32
Comment: ACH personnel should be reassigned to another department or have their access levels restricted from transaction posting upon notification they are resigning from the credit union.

Cell: B34
Comment: NACHA rules require credit unions to obtain an internal or external audit of their ACH function from a qualified individual not involved in the ACH operation annually. The audit should assess compliance with ACH rules and needs completed no later than December 1 of each year. The credit union must retain ACH audit documentation for a period of six years.

Cell: B42
Comment: The credit unions enterprise-wide BCP plan should include strategies for restoring ACH functions in the event of a disaster or disruption of service. Credit unions do not need to have a separate BCP plan for ACH. The level of detail in the business continuity plan will be dependent on factors such as size and complexity of the credit union, ACH services offered, and third-party service agreements. The plan should adequately address RDFI and if applicable ODFI functions.

Cell: B43

Comment: ACH operations are reliant on both computer systems and communications lines. ACH strategies should address not only full failures of computer systems and communications lines but also partial failures. Both types of failures can cause the inability to process ACH activity. The inability to process ACHs could increase the reputation risk of the credit union.

Cell: B44
Comment: BCP recovery strategies should be appropriate for the size of the credit union in relation to the services it offers and the volume of its activity. For example, a large credit union should have adequate financial resources to maintain a backup facility with redundant operations while a smaller credit union may have a reciprocal agreement with another credit union or rely on a corporate credit union.

Cell: B49
Comment: NACHA Rules require the retention of all entries, including return and adjustment entries, transmitted to and received for a period of six years after the date of transmittal.

	A	B	C	F
3	**ACH - Receiving Depository Financial Institution**			
4	**INTRODUCTION AND PURPOSE**			
5	**ABBREVIATIONS**			
6	**NCUA REFERENCES**			
7	**EXTERNAL REFERENCES**			
8			**Yes/No/NA**	**Comments**
9	1.0.0	Does the credit union examine each prenotification entry to verify it contains a valid open account number and correct account type?		
10	1.1.0	Does the credit union send Notification of Changes (NOC) to correct incorrect information received on initial entries for recurring transactions?		
11	1.2.0	Does the credit union accept the first ACH information received for a transaction which contains an account number as shown on the MICR line on the bottom of share drafts or similar instruments?		
12	1.3.0	Does the credit union warehouse credit and debit entries received prior to the settlement date?		
13	1.4.0	Does the credit union post warehoused credit and debit entries received on the settlement date?		
14	1.5.0	Does the credit union as an RDFI freeze proceeds of ACH transactions of blocked parties pending guidance from OFAC?		
15		**Credits:**	**Yes/No/NA**	**Comments**
16	2.0.0	Does the credit union ensure staff follows appropriate rules and procedures to ensure the availability of funds in accordance with:		
17	2.0.1	NACHA Rules requiring funds to be available by opening of business or 9:00 a.m. the day of settlement for Pre-arranged payment and deposit entry (PPD) and pre-arranged payment credits?		
18	2.0.2	Federal Government requirements for benefit and salary payments?		
19		**Debits:**	**Yes/No/NA**	**Comments**
20	3.0.0	Do the credit union procedures require timely return of debits received for accounts with insufficient funds?		
21	3.1.0	Are the credit union ACH operating personnel aware of and do they comply with ACH return deadlines for all ACH return items?		
22	3.2.0	Does the credit union research and identify correct account numbers for posting of debit transactions rejected for incorrect account number (NACHA requirement)?		
23	3.3.0	Does the credit union contact members to determine if a returned debit items is a "Stop payment" or an "Unauthorized Debit"?		
24	3.4.0	If the item is a PPD debit not authorized by the member, are ACH personnel required to secure a signed affidavit from the member before returning the item, as required by the NACHA Rules?		
25	3.5.0	Are all ACH personnel familiar with the different rules for returns for various Standard Entry Class Codes?		
26	3.6.0	Does the credit union have procedures to ensure it applies the proper Return Reason Codes for returns?		

Cell: A4

Comment: The RDFI Tab is designed to assess the risks associated with credit unions who act as receiving depository financial institutions and originate only their return items. If the credit union is originating any transactions other than returns, please complete the ODFI-Moderate and ODFI-High Tabs as applicable.

Cell: A5

Comment: Abbreviations and Definitions:

ACH - Automated Clearing House
ACH Credits – an ACH transaction which an originator initiates to move funds to a Receiver's account.
ACH Operator - The central clearing facility operated by EPN, a private organization, or the Federal Reserve Bank.
MICR (Magnetic Ink Carriage Return Line) - Magnetically encode line on the bottom of a check.
NACHA - National Automated Clearing House Association
NOC (Notification of Change) - Notification to a merchant from a customer's financial institution indicating the bank account information provided with a specific transaction is incorrect.
OFAC - Office of Foreign Asset Control
Originator – The entity that arranges with an RDFI for ACH entries to be entered into the payment system. An originator may be a company or a consumer.
Originating Depository Financial Institution (ODFI) - A participating financial institution that originates ACH entries at the request of and by agreement with its customers.
PPD (Pre-arranged payment and deposit entry) - The alphabetic mnemonic used to identify credit or debit entries initiated by an originator pursuant to a standing or single-entry authorization from its customer or employee.
Receiving Depository Financial Institution (RDFI) - A financial institution that provides depository account services to consumers, employees, and businesses and accepts electronic debits and credits to and from those accounts. Any financial institution qualified to receive ACH entries that agrees to abide by the NACHA Operating Rules and Guidelines.
Receiver - The person or corporate entity that has authorized a merchant to initiate a refund or charge transaction to their bank account.
Receiving Point - A site where entries are received from an ACH Operator for processing. It may be the RDFI, its data center or a data processing service bureau authorized to receive entries on behalf of a RDFI. Corporate credit unions act as a receiving point on behalf of natural person credit unions.
Sending Point - A processing site from which entries are transmitted to the ACH operator. If may be the ODFI on its own behalf or a financial institution or private data processing service bureau on behalf of the ODFI. Corporate credit unions act, in some instances, as sending points for natural person credit unions.

Cell: A6

Comment: Letter to CU 170-05-95 Automated Clearinghouse - Deposits for Processing Activities

Cell: A7

Comment: (1) NACHA Rules
(2) Treasury Department's Green Book - Rules governing Federal Government payments and reclamations.
(3) FFIEC's Bank Secrecy Act/Anti-Money Laundering Act Examination Guide
(4) 12 CFR Part 205 - Regulation E - Federal Regulation governing consumer electronic transfers/payments.
(5) Title 31 CFR Part 210 - Rules governing Federal Government payments.
(6) FRB Operating Circular 4 and its sub circulars/appendices- Federal Reserve operating circular governing the clearing and settlement of commercial ACH credit and debit items.
(7) 26 CFR Parts 1, 20, 25, 31, and 40 - Federal Regulation governing electronic funds transfers of Federal deposits.

Cell: B9

Comment: Prenotification - A prenotification is a non-dollar entry sent through the ACH Network by an Originator to the RDFI. It conveys the same information (with the exception of the dollar amount and transaction code) that will be carried on subsequent entries, and it allows the RDFI to verify the accuracy of the account data. Use of the prenotification process by an Originator is optional for all standard entry class codes. Although the use of prenotifications is optional for originators, RDFI's need to understand that by sending a prenotification, the originator is shifting some liability to the RDFI, therefore the RDFI must verify the account information for all prenotifications it receives. The RDFI must verify account number information and should also verify the account type (savings vs. checking, etc). According to

NACHA rules, if the individual name on the entry is not the name on the account, the RDFI can rely solely on the account number for posting purposes. When an institution receives prenotifications, it has three options:
1. Accept the prenotification if the account information is correct. No further action is required.
2. Notify the originator that it will not accept the live entry by returning the prenotification. The information on the prenotification is incorrect and the correct information is not available.
3. Notify the originator by originating a notification of change that it will accept the live entries, but certain information is incorrect and needs to be changed on the subsequent live entry(ies).

Cell: B11
Comment: Accepting account information on the first entry received allows for the conversion of check items to ACH entries. Large credit unions can have separate routing numbers for ACH and share draft items. Credit unions must accept and be able to process converted items per electronic check conversion regulations.

Cell: B12
Comment: ACH entries are sent in advance of their settlement date. Credit union computer systems or third party data system processors must have the ability to "warehouse" or store the entries for processing on their settlement date.

Cell: B14
Comment: OFAC sanctions require transactions for blocked parties to be frozen or held pending guidance or release under OFAC direction.

Cell: B18
Comment: References:
[31 CFR Part 217.7(d)] and Treasury Department's Green Book.

Cell: B20
Comment: To limit a credit union's liability, returns must be processed the day following settlement. Certain types of returns can be processed up to 60 days from receipt.

General return time frames are as follows:

NSF, account closed, unable to locate account, invalid account number, payment stopped, uncollected funds, beneficiary or account holder deceased, and account frozen must be returned no later than the day after settlement. Most items are returned the day of settlement because automated posting allows for the items to be processed quicker.

Returns for unauthorized debit, authorization revoked, or customer advises not authorized may be processed up to 60 days from date of receipt. Additionally, an entry of a deceased account holder "deceased" may be returned up to 60 days from receipt. Normally, once a credit union is notified a member is deceased, the account is coded "deceased" and any future entries automatically generate an exception for return processing.

Cell: B21
Comment: The credit union should have a NACHA rules book and staff should be aware of and trained on time frames.

Cell: B23
Comment: A "Stop payment" is a one time stop for a recurring debit. An "Unauthorized debit" is a debit not originally authorized by the member. Different return reason codes are needed for these items, therefore it is important the credit union require the appropriate affidavit from the member to support their return.

Cell: B26
Comment: There are numerous Return Reason Codes. Each Return Reason Code is meant for a specific type of transaction or incident and they are not interchangeable. The ODFI can reject a return if an incorrect Return Reason Code is used and the RDFI would incur unnecessary liability for the transaction.

	A	B	C	E
3	**Origination Depository Financial Institution - Moderate Risk**			
4	**INTRODUCTION AND PURPOSE**			
5	**ABBREVIATIONS AND DEFINITIONS**			
6	**REFERENCES**			
7	**EXTERNAL REFERENCES**			
8		**ODFI - General**	**Yes/No/NA**	**Comments**
9	1.0.0	Do employees responsible for the ACH operation receive initial and annual training on the requirements of NACHA rules regarding originations, including proper authorization, liabilities, warranties, etc.?		
10	1.1.0	Does the credit union have a written agreement with each Originator that warrants adherence to the NACHA Rules? (NACHA Rules, Article Two - 2.1.1)		
11	1.2.0	Has the credit union offered security procedures to each Originator that transmits entries subject to the Uniform Commercial Code (UCC) Section 4A-201?		
12	1.3.0	Has the the credit union established daily transaction limits for member originations?		
13		**ACH Origination-General**	**Yes/No/NA**	**Comments**
14	2.0.0	1. Does the credit union use any third party processor to send ACH transactions directly to the ACH Operator? If yes, provide the names in the Comments column.		
15	2.1.0	2. Does the credit union have procedures to verify the origination transaction limits are not exceeded and the origination request is authorized?		

Cell: B4
Comment: The ODFI-Moderate tab is designed to assess the risk and controls over credit unions which originate member loan payment transactions and member to member transfers through the ACH network. If the credit union is originating payroll for its member businesses, the ODFI-High Tab should be completed.

Cell: A5
Comment: The ACH Network is a batch processing, store-and-forward system. Transactions received by the credit union during the day are stored and processed later in a batch mode. Rather than sending each payment separately, ACH transactions are accumulated and sorted by destination for transmission during a predetermined time period. This provides significant economies of scale. It also provides faster processing than paper checks, which must be physically handled. Instead of using paper to carry necessary transaction information, ACH transactions are transmitted electronically between financial institutions through data transmission.

Definitions of the Participants:
Originator – The originator is the entity that agrees to initiate ACH entries into the payment system according to an arrangement with a Receiver. An originator may be either a company or a consumer.
Originating Depository Financial Institution (ODFI) is the institution that receives payment instructions from Originators and forwards the entries to the ACH Operator. An ODFI may participate in the ACH system as a RDFI without acting an ODFI; however, if the ODFI chooses to originate ACH entries, it must also agree to act as an RDFI. The ODFI warrants the accuracy and validity of every transaction.
ACH Operator is the central clearing facility operated by a private organization or a Federal Reserve Bank.
Receiving Depository Financial Institution (RDFI) receives the ACH entries from the ACH Operator and posts the entries to the accounts of its depositors (receivers).
Receiver - A Receiver is a natural person or organization which has authorized an Originator to initiate an ACH entry to the Receiver’s account with the RDFI. A Receiver may be either a company or a consumer, depending on the type of transaction.
ACH Credits – an originator initiates a transfer to move funds into a Receiver’s account.
ACH Debit - an originator initiates a transfer which removes funds from a Receiver's account.

The ACH Network supports a variety of payment applications. Each ACH application is identified and recognized by a specific three-digit code, know as a Standard Entry Class Code (SEC Code) which appears in the ACH record format. The TEL (Telephone Initiated Entry) is used for the origination of a single entry debit transaction to a consumer’s account pursuant to an oral authorization.

Cell: A6
Comment: (1) NACHA Rules
(2) Treasury Department's Green Book - Rules governing Federal Government payments and reclamations.
(3) FFIEC's Bank Secrecy Act/Anti-Money Laundering Act Examination Guide
(4) 12 CFR Part 205 - Regulation E - Federal Regulation governing consumer electronic transfers/payments.
(5) Title 31 CFR Part 210 - Rules governing Federal Government payments.
(6) FRB Operating Circular 4 and its sub circulars/appendices- Federal Reserve operating circular governing the clearing and settlement of commercial ACH credit and debit items.
(7) 26 CFR Parts 1, 20, 25, 31, and 40 - Federal Regulation governing electronic funds transfers of Federal deposits.

Cell: A7
Comment: (1) NACHA Rules
(2) Treasury Department's Green Book - Rules governing Federal Government payments and reclamations.
(3) FFIEC's Bank Secrecy Act/Anti-Money Laundering Act Examination Guide
(4) 12 CFR Part 205 - Regulation E - Federal Regulation governing consumer electronic transfers/payments.
(5) Title 31 CFR Part 210 - Rules governing Federal Government payments.
(6) FRB Operating Circular 4 and its sub circulars/appendices- Federal Reserve operating circular governing the clearing and settlement of commercial ACH credit and debit items.
(7) 26 CFR Parts 1, 20, 25, 31, and 40 - Federal Regulation governing electronic funds transfers of Federal deposits.

Cell: B10
Comment: Agreement should address:
1) Liabilities and Warranties,
2) Responsibilities for processing arrangements, and
3) Other originator obligations such as security and audit requirements.

Cell: B11
Comment: UCC-4A-201 states the following:

"Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.

Cell: B12
Comment: This is a best practice recommendation. Implementation of a daily transaction limit allows the credit union to monitor member activity in conjunction with a credit review analysis of ACH operations. Software should have the capability to establish maximum daily limits which would reduce liability and the chance of releasing fraudulent or unauthorized transactions. Limit also provides management another tool for cash management and reduces the potential of accessing the line of credit on the settlement account or overdrawing the Federal Reserve Account.

Cell: B14
Comment: Corporate credit unions can offer the ability to process ACH transactions through their online ACH program which is accessible via their home banking solution. The credit union should have an agreement with the corporate or other third party processor outlining their responsibilities and liabilities.

Cell: B15
Comment: This is generally accomplished by invoking dual controls. The corporate "home banking" solution for ACH typically established two administrative users who are responsible for setting up the credit unions users. Credit union's should check the options for dual control requiring a second individual to verify transactions entered for uploading and the release files.

	A	B	C	E
3	**Originating Depository Financial Institution - High Risk**			
4	**INTRODUCTION AND PURPOSE**			
5	**ABBREVIATIONS AND DEFINITIONS**			
6	**REFERENCES**			
7	**EXTERNAL REFERENCES**			
8		**Policies and Procedures**	**Yes/No/NA**	**Comments**
9	1.0.0	Are policies and procedures in writing and approved by the board of directors or a designated committee, if applicable?		
10	1.1.0	Do policies and procedures adequately address Originating Depository Financial Institution (ODFI) responsibilities?		
11	1.2.0	Does the policy include the process management will utilize to monitor activity, returns, and known and potential fraudulent activity?		
12	1.3.0	Does the policy include a process for monitoring compliance with NACHA rules, Uniform Commercial Code (UCC)-4A, state and Federal laws including BSA and OFAC?		
13	1.4.0	Does the policy include a mechanism for periodic reviews and updates?		
14	1.5.0	Does the credit union have adequate procedures to verify the Originator is authorized and their exposure limits are not exceeded?		
15	1.6.0	Does the credit union have procedures to notify the appropriate officer if a file is received for ACH input which exceeds the established exposure limit for override or denial?		
16	1.7.0	Does the credit union have documented instructions for processing incoming and outgoing ACH items that include appropriate second party reviews and segregation of duties?		
17	1.8.0	Does the credit union have specific procedures in place in the event of a security breach?		
18	1.9.0	Does the credit union's incident response program address ACH activity?		
19		**Agreements**	**Yes/No/NA**	**Comments**
20	2.0.0	Does the credit union have a written agreement with each Originator that warrants adherence to the NACHA Rules?		
21	2.1.0	If Cash Concentration or Disbursement (CCD) or Corporate Trade Exchange (CTX) entries are originated, how has the credit union verified the Receiver has agreed with the Originator to be bound by NACHA Rules?		
22	2.2.0	Has the credit union offered commercially reasonable security procedures to each Originator that transmits entries subject to UCC-4A?		
23	2.3.0	Does the agreement stipulate reserve or compensating balance requirements for pre-funding? If not, does it require a line of credit?		

	A	B	C	E
3	**Originating Depository Financial Institution - High Risk**			
24	2.4.0	Does the agreement establish standard operating procedures for file acceptance times, requirements to accept returns, and compliance with security procedures?		
25	2.5.0	Does the credit union have an agreement with each Originator that excuses the credit union for failure to perform due to natural and other disasters?		
26	2.6.0	Does the agreement address exposure limits?		
27	2.7.0	Does the agreement provide for a separate limit for WEB, TEL, or other high risk entries?		
28	2.8.0	Does the agreement include provisions for GLBA?		
29		**ACH Funding and Credit Risk**	**Yes/No/NA**	**Comments**
30	3.0.0	Does the credit union obtain assurances that sufficient collected funds or lines of credit are available before releasing transaction to the ACH operator?		
31	3.1.0	Does the credit union block or hold funds until the transaction settlement date for member business accounts with pre-funding arrangements,?		
32	3.2.0	For member business accounts with non-pre-funded arrangements, does the credit union:		
33	3.2.1	Place a block or hold funds in a deposit account?		
34	3.2.2	Reduce the available funds balance of the line of credit prior to or at the time of origination?		
35	3.3.0	Does management approve extensions of lines of credit or draws against uncollected funds before origination of transactions?		
36	3.4.0	Is documentation retained supporting the approval?		
37	3.5.0	Are ACH debit origination deposits treated as uncollected funds?		
38	3.6.0	Does the credit union monitor draws against uncollected funds for high risk member business accounts?		
39	3.7.0	Does management approve draws against uncollected ACH deposits and maintain documentation to support approval for high risk customers?		
40	3.8.0	Are credit assessments performed for member business accounts originating ACH transactions?		
41	3.9.0	Does the credit union assess and manage credit risk by evaluating and ranking the Originator’s total exposure as an unsecured line of credit?		
42	3.10.0	Does a loan officer review, approve, and set exposure limits for new ACH credit entry Originators?		
43	3.11.0	Does the ACH department monitor exposure limits for each Originator across multiple settlement dates?		
44	3.12.0	Does the credit union require pre-funding before originating transaction for Originators with an inadequate exposure limit for their type of origination?		
45	3.13.0	Does the credit union place limits on the amount of debits originated?		
46	3.14.0	Are credit assessments periodically updated to evaluate possible changes to a member business account's creditworthiness, financial condition and economic conditions?		

	A	B	C	E
3	**Originating Depository Financial Institution - High Risk**			
47	3.15.0	Has management included an analysis of ACH services daily, weekly, and monthly funding requirement in the overall evaluation of the credit union's liquidity needs?		
48		**WEB & TEL Entries - CU Originated**	**Yes/No/NA**	**Comments**
49	4.0.0	Does the credit union adhere to NACHA guidelines for originating WEB or TEL entries?		
50	4.1.0	Is adequate consumer authentication and authorization obtained?		
51	4.2.0	Does the credit union provide written consumer notices, prior to the settlement date, confirming the terms of the authorization?		
52	4.3.0	Does the credit union record all oral authorizations?		
53	4.4.0	Does the credit union monitor return rates by transaction type and originator?		
54		**WEB & TEL Entries - Mbr Business Acct Originated**	**Yes/No/NA**	**Comments**
55	5.0.0	Are the credit union's policies and procedures adequate for business accounts and transactions involving Internet-initiated (WEB) and telephone-initiated (TEL) entries?		
56	5.1.0	Does the credit union adhere to NACHA guidelines concerning merchant management and their business practices?		
57	5.2.0	Does the credit union monitor return rates by transaction type and originator?		
58		**Member Business Acct Originated**	**Yes/No/NA**	**Comments**
59	6.0.0	Does the credit union originate payrolls for member businesses?		
60	6.1.0	Do written ACH policies authorize the origination of member business payrolls?		
61	6.2.0	Do written ACH policies specify whether pre-funding is required for origination of ACH payrolls?		
62	6.3.0	Does the credit union require the member business originator to pre-fund for payroll originations? If not, why does the credit union not require pre-funding?		
63	6.4.0	Does the credit union limit ACH based credit exposure for originated payrolls to multiples of net worth based on member business creditworthiness?		
64	6.5.0	Would the origination of an ACH Transaction for a member business payroll, that is not pre-funded, result in a dollar amount that exceeds the unsecured Member Business Loan Limit in the NCUA RR 723.7(c)(2) in the event funding does not occur on the day of		
65	6.6.0	Are credit assessments performed for member business accounts originating ACH transactions for a member business payroll?		
66	6.7.0	Are credit assessments periodically updated to evaluate possible changes to a member business account's creditworthiness, financial condition and economic conditions?		

	A	B	C	E
3	**Originating Depository Financial Institution - High Risk**			
67	6.8.0	Does the ACH department monitor exposure limits for each member business account who originates ACH payrolls across multiple settlement dates?		
68	6.9.0	Does the credit union require pre-funding before originating transaction for Originators with an inadequate exposure limit for their type of origination?		
69		**Cross Border and International ACH Transactions**	**Yes/No/NA**	**Comments**
70	7.0.0	Does the credit union process cross border (CBR) or international (IAT) ACH transactions?		
71	7.1.0	If yes, does the credit union maintain a list of countries it sends ACH files to as an ODFI?		
72	7.2.0	Does the credit union track or trend CBR and/or IAT ACH originations by the recipient country?		
73	7.3.0	Does the credit unions as the ODFI check all ACH fields (Originator and Receivers) against the OFAC SDN list prior to sending the ACH file?		

Cell: A4

Comment: This questionnaire is designed for credit union's which pose a higher ACH risk because of their type of ACH origination activity. This questionnaire should be completed for credit union's originating transactions for members with business accounts, ACH Payroll originations, Cross Border and International ACH transactions, CUSOs, or high risk ACH transactions such as WEB or TEL.

Cell: A5

Comment: The ACH Network supports a variety of payment applications which are identified and recognized in the ACH record format by a specific three-digit code, known as a Standard Entry Class Code (SEC Code).

TEL – Telephone Initiated Entry is used for the origination of a single entry debit transaction to a consumer’s account pursuant to an oral authorization.
WEB - Electronic authorization through the Internet to identify debit entries initiated by an Originator pursuant to an authorization obtained from the Receiver to initiate a transfer of funds from a Receiver's account.

Cell: A6

Comment: (1) NACHA Rules
(2) Treasury Department's Green Book - Rules governing Federal Government payments and reclamations.
(3) FFIEC's Bank Secrecy Act/Anti-Money Laundering Act Examination Guide
(4) 12 CFR Part 205 - Regulation E - Federal Regulation governing consumer electronic transfers/payments.
(5) Title 31 CFR Part 210 - Rules governing Federal Government payments.
(6) FRB Operating Circular 4 and its sub circulars/appendices- Federal Reserve operating circular governing the clearing and settlement of commercial ACH credit and debit items.
(7) 26 CFR Parts 1, 20, 25, 31, and 40 - Federal Regulation governing electronic funds transfers of Federal deposits.

Cell: A7

Comment: (1) NACHA Rules
(2) Treasury Department's Green Book - Rules governing Federal Government payments and reclamations.
(3) FFIEC's Bank Secrecy Act/Anti-Money Laundering Act Examination Guide
(4) 12 CFR Part 205 - Regulation E - Federal Regulation governing consumer electronic transfers/payments.
(5) Title 31 CFR Part 210 - Rules governing Federal Government payments.
(6) FRB Operating Circular 4 and its sub circulars/appendices- Federal Reserve operating circular governing the clearing and settlement of commercial ACH credit and debit items.
(7) 26 CFR Parts 1, 20, 25, 31, and 40 - Federal Regulation governing electronic funds transfers of Federal deposits.

Cell: B9

Comment: A well defined policy will include:
(1) The regulatory framework governing ACH operation;
(2) The authorized types of ACH activity (ODFI, RDFI) including a listing of the specific transaction types;
(3) The members and/or member business account authorized to participate in ACH originations;
(4) A definition of the credit union's RDFI and ODFI responsibilities;
(5) The acceptable level of risk for ACH activities and risk mitigation controls (internal controls);
(6) The credit underwriting standards to establish origination debit and credit limits;
(7) The acceptable time period for re-evaluation of originator financial condition and credit worthiness;
(8) The credit unions requirement for originators to pre-fund versus use of an established line of credit;
(9) A description of the ACH monitoring process performed across multiple settlement days to comply with NACHA rules;
(10) The initial and annual training programs required to be completed by ACH personnel to ensure compliance with required rules and regulations;
(11) The management oversight program which ensure compliance with applicable consumer protection and Federal regulations;
(12) The credit unions policy to comply with ACH audit and records retention requirements; and
(13) The Business Continuity/Disaster Recovery Plan to recover ACH operations.

Policies/procedures need expanded if the credit union initiates WEB and TEL transactions because NACHA has specific processing requirements. For example, TEL transactions must be recorded, provide for processes to reasonable identify member(s) authorizing the transaction, and require written confirmation of the transaction prior to the settlement day. WEB transaction should include a strong authentication process to ensure identification of the member authorizing the transaction.

Policies should be approved by the Board of Directors to ensure directors approve the level of ACH origination risk proposed by management is acceptable.

Cell: B10
Comment: ODFI responsibilities vary by the type of ACH activity/transactions and the mitigating controls implemented by the credit union. For example, the operating procedures of requiring prenotifications for all origination activity mitigates some originating risk by shifting responsibility to the RDFI. The RDFI is required to inform the ODFI if the account information is correct.

Cell: B11
Comment: Best Practice. Originators not verifying the individual and/or information for transaction could result in a excessive volumes of fraudulent returns. This could result in the credit union being fined for non-compliance with NACHA rules.

Cell: B12
Comment: Article 4A creates a series of rules to govern the resolution of legal issues that may arise out of funds transfers. ACH transfers and other funds transfers that are not subject to Regulation E are subject to Article 4A of the Uniform Commercial Code. This article applies to the sending and receiving of ACH and wire transfers, payment orders provided to depository institutions, crediting and settlement of funds, and disclosure requirements.

Cell: B14
Comment: Best Practice - ACH software usually permits credit unions to enter established exposure limits into each account holders profile to monitor and control their debit and credit activity. Software controls prevents files of origination activity from being released with supervisory authority. Most software includes the capability to generate a report showing all originators which exceeded their exposure limits. This report should be provided to the ACH supervisor and the credit analyst. The credit analyst, after a credit review, could recommend to the ACH department a temporary credit increase or to suspend the file(no release of the file). The suspension of a file requires the credit union to notify the originator the reason for the suspension.

Cell: B17
Comment: Procedures for ACH software/file breaches should be similar to IT security breaches.

Cell: B21
Comment: CCD- Cash Concentration or Disbursement - The alphabetic mnemonic to identify debits or credits initiated by an originator to consolidate funds from its branches, agents or from other organizations. CCD's can be either a credit or debit where funds are either distributed or consolidated between corporate entities.

CTX- Corporate Trade Exchange - The alphabetic mnemonic to identify credit or debit entries originated by an originator to pay or collect on an obligation of the originator to the account of another organization. CTX supports the transfer of funds (debit or credit) within a trading partner relationship.

These entries would be initiated by the credit union for automated posting to the member accounts originating activity.

Cell: B22
Comment: UCC-4A-201 states the following:

"Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.

Cell: B27
Comment: WEB and TEL transaction are higher risk transactions prone to abuse and fraudulent activity. By establishing separate debit and credit origination limits for these transactions, the credit union limits its potential liability to fraudulent activity. Most ACH origination software will allow the user to define limits by transaction type.

Cell: B28
Comment: GLBA - Gramm Leach Bliley Act - Protection of consumer information. This is a standard contract provision and should be included to ensure originators understand the information is protected under Federal Law and as such, information should be treated as confidential.

Cell: B30
Comment: Collected funds includes funds on deposit or pre-funding requirements.

Cell: B32
Comment: A non-pre-funded arrangement exists for a member when they have a settlement line of credit or the member credit worthiness is excellent and the credit union determines the default risk on their ACH activity is low. Best practices for non-pre-funded arrangements is to require the member to have a settlement line of credit. Originating ACH activity without pre-funding or a settlement line of credit should not occur because it increases default risk.

Cell: B41
Comment: The evaluation should consider at least whether:
1) The limit is based on the originator's credit rating and activity levels.
2) The limit is based on board approved policy.
3) The limit is reasonable relative to the originator’s exposure across all services (lending, cash management, etc.).
4) The limits have been established for originators whose entries are transmitted to the ACH operator by a service provider.
5) A written agreement addressing exposure limits is in place with originators.
6) A separate limit for WEB & TEL entries and other high-risk ACH transactions has been established.

Cell: B43
Comment: NACHA rules require ODFI's to monitor exposure limits across multiple settlement days. A credit union has exposure and responsibility for transactions for a minimum of two business days, but certain ACH transactions may be returned for up to 60 days. Transactions are normally sent to receivers in advance of their settlement date and warehoused by the receiver for posting on the settlement date. Pre-funding is not required for all types of activity, so the credit unions risk exposure increases during this period. A conservative organization would monitor exposure for up to 60 days, however the standard practice is to monitor for at least two business days.

Cell: B46
Comment: Best practice - Originators financial condition can change quickly no matter the size, type, or maturity of the business. Business deposit accounts should be reviewed periodically to monitor changes in cash flow. A company which experiences a significant change in their cash flow should have its exposure limit reduced, require collateral, or require pre-funding.

Cell: B47
Comment: Origination of ACH debit and credit transactions can impact a credit union liquidity. Management should understand the impact of the dollar volume of ACH activity in relation to its daily, weekly and monthly funding

needs. Strong cash management practices need to be in place to mitigate overdrafts at the Federal Reserve or corporate credit union.

Cell: B51
Comment: For TEL entries, the consumer must receive a written notice summarizing the telephone authorization to include the account to be debited, the amount and date their account will be debited. The notice must provide the consumer with information on who to call to dispute/cancel the transaction.

Cell: B52
Comment: Recording may be done electronically through a computerized telephone system or on tape.

Cell: B55
Comment: Policies/procedures need expanded if the credit union initiates WEB and TEL transactions because NACHA has specific processing requirements. For example, TEL transactions must be recorded, provide for processes to reasonable identify member(s) authorizing the transaction, and require written confirmation of the transaction prior to the settlement day. WEB transaction should include a strong authentication process to ensure identification of the member authorizing the transaction.

Cell: B64
Comment: Part 723.7(c) of the NCUA RR states “You may make unsecured member business loans under the following conditions:
(1) You are a natural person credit union that is well capitalized as defined by § 702.102(a)(1) of this chapter or you are a corporate credit union that maintains a minimum capital ratio as required by § 704.3(d) of this chapter or a different ratio as permitted under § 704.3(e) of this chapter;
(2) The aggregate of the unsecured outstanding member business loans to any one member or group of associated members does not exceed the lesser of $100,000 or 2.5% of your net worth; and
(3) The aggregate of all unsecured outstanding member business loans does not exceed 10% of your net worth."

Cell: B67
Comment: The evaluation should consider at least whether:
1) The limit is based on the originator's credit rating and activity levels.
2) The limit is based on board approved policy.
3) The limit is reasonable relative to the originator’s exposure across all services (lending, cash management, etc.).
4) The limits have been established for originators whose entries are transmitted to the ACH operator by a service provider.
5) A written agreement addressing exposure limits is in place with originators.
6) A separate limit for WEB & TEL entries and other high-risk ACH transactions has been established.

Cell: B73
Comment: For domestic ACH files, ODFI's are only responsible to check the Originators against the SDN list, but for international ACH transmissions, the ODFI must check all names against the SDN list.

	A	B	C	E
3	**WIRE TRANSFER CONTROLS**			
4	**INTRODUCTION AND PURPOSE**			
5	**EXTERNAL REFERENCES**			
6		**General**	**Yes/No/NA**	**Comments**
7	1.0.0	Does the credit union have wire transfer capabilities at more than one location?		
8	1.1.0	Do the branches have wire transfer capabilities? If yes, document the branches in the comments section.		
9	1.2.0	What wire transfer system does the credit union use?		
10	1.3.0	Does the credit union have a written organization plan indicating the structure of the wire transfer and securities transfer departments?		
11	1.4.0	Does management regularly review staff compliance with personnel procedures, operating instructions, and internal control?		
12	1.5.0	Has the credit union developed a formal audit program that covers all aspects of the wire transfer area?		
13	1.5.1	Has the audit staff been formally trained in the communication systems, operations, and controls necessary for a wire transfer operation?		
14	1.5.2	Has an annual audit (internal or external) of the area been performed?		
15	1.6.0	Does the credit union have written procedures for all types of wire requests, including: Investment wires, Third Party wires, and Foreign wires?		
16	1.7.0	Is a log maintained for all wire transfers (incoming and outgoing) done on a daily basis?		
17		**Agreements**	**Yes/No/NA**	**Comments**
18	2.0.0.	Are agreements relating to wire transfer operations in effect between the credit union, its equipment suppliers, members, and/or Federal Reserve Bank, Corporate Credit Union, third party vendor.?		
19	2.0.1	Are all agreements current?		
20	2.0.2	Do the agreements fix responsibility and accountability between the parties?		
21		**Transfer Requests**	**Yes/No/NA**	**Comments**
22	3.0.0	Does the credit union have written procedures for its employees to positively identify members requesting wire transfers?		
23	3.0.1	Is a standard form used for all requests?		
24	3.0.2	Are telephone requests tape recorded (suggested)?		
25	3.0.3	How long are the recordings maintained?		
26	3.0.4	Are the recordings stored in a controlled area?		
27	3.0.5	Is the data repeated to the member making the call to verify information?		
28	3.1.0	Is there a procedure for call back verification of telephone requests?		
29	3.2.0	Is the member's telephone number of record used for call back verifications? If not, comment on verification procedures.		
30		**Contingency Planning**	**Yes/No/NA**	**Comments**
31	4.0.0	Is there a current written BCP/DR contingency plan?		

	A	B	C	E
3	**WIRE TRANSFER CONTROLS**			
32	4.1.0	Are employees familiar with contingency plan procedures and are they periodically tested?		
33		**Personnel**		
34	5.0.0	Does the credit union have a policy restricting any relatives of wire transfer employees from working in the accounting or data processing department?		
35	5.1.0	Is there a formal training program emphasizing security and control?		
36	5.2.0	Does management transfer employees assigned to the fund transfer department to another department or remove their capability to process wire transfers when notice of their resignation is received?		
37	5.3.0	Is the terminated employee's access rights to funds transfer software and hardware removed promptly?		
38	5.4.0	Is there a background check, which is documented (police, bond, credit checks), performed on individuals before they are assigned to the wire unit?		
39	5.5.0	Are employees with wire transfer capabilities subject to unannounced rotation of responsibilities?		
40	5.6.0	Are employees required to take at least 5 consecutive days of vacation and is another employee required to complete the Wire Transfer duties?		
41	5.6.1	(a) Is the policy being enforced?		
42		**Processing**	**Yes/No/NA**	**Comments**
43	6.0.0	Are verification procedures used to validate the member and transfer information prior to final execution?		
44	6.1.0	Is there separation of duties in receipt, initiation, verification, transmission, and reconciliation of transfers?		
45	6.2.0	Does each employee initial the transfer forms to designate the process each performs?		
46	6.3.0	Is the member's account balance checked before making the transfer?		
47	6.4.0	Are forms sequentially numbered on all transfers?		
48	6.5.0	Is the supervisor promptly notified of any suspicious irregularities in transactions?		
49	6.6.0	Are printed copies of transfers checked for correctness of transmission?		
50	6.7.0	Are transactions documented for proper audit trail?		
51		**Balancing**	**Yes/No/NA**	**Comments**
52	7.0.0	Is transfer activity balanced periodically during the day?		
53	7.1.0	Do the balancing procedures account for all transfers in a final proof?		
54	7.2.0	Are transfer advices reconciled to account entries on a daily basis?		
55		**Wire Unit Controls**	**Yes/No/NA**	**Comments**
56	8.0.0	Number of employees with physical access to the wire transfer terminal		
57	8.1.0	Does management review wire transfer reports on a periodic basis which documents wire transfer activity for each authorized employee? Have reports been made available that determine appropriate limits, authorized access levels and separation of duties?		
58	8.2.0	Are these reports reviewed and updated periodically?		

	A	B	C	E
3	**WIRE TRANSFER CONTROLS**			
59	8.3.0	Is there a requirement to have changes in employee fund transfer limits properly authorized before changes are made in the software?		
60		**Audit**	**Yes/No/NA**	**Comments**
61	9.0.0	Does the annual audit include a review of the wire transfer operation of the credit union?		
62	9.1.0	Do the audit steps include a review of insider accounts (i.e., the review should include the origination and/or receipt of wire transfers)?		
63	9.2.0	Does the internal auditor or supervisory committee periodically review insider account activity related to wire transfers?		

Cell: B4

Comment: This questionnaire should be used to determine the adequacy and effectiveness of the security controls and business continuity planning for the credit union's funds transfer application. These procedures evaluate the effectiveness of the credit union's control environment and related risk management processes for the funds transfer application.

The usage of these examination procedures should be based on the examiner's assessment of the risks and risk management practices related to the credit union's wire operations, including transaction volumes. This assessment should include consideration of formal policies and procedures, as well as an assessment of the effectiveness of the credit union's overall information security and business continuity planning.

If the credit union uses Fedline Advantage for wire transfers, examiner should consider completing the Fedline Advantage questionnaire.

Cell: B5

Comment: Federal Reserve Board Operating Circulars OC-4, OC-5, and OC-6 which can be found on line at: http://www.frbservices.org/OperatingCirculars/index. html

Cell: B9

Comment: Credit union can use the Federal Reserve, Corporate Credit Union, local bank, or third party vendor for wire transfer capabilities. If FedLine Advantage used for wire transfers, consider completing the FedLine Advantage questionnaire.

Cell: B12

Comment: The formal audit program should cover, at a minimum, the following:

a) Review of written policies and procedures for accepting and initiating wire transfers;

b) Determining if an accurate list of persons authorized to initiate funds transfers are maintained;

c) Documentation that the wire transfer process was observed especially the morning log-on procedures;

d) Review of daily settlement debits and credits which includes the tracing of all or a sample of figures to source documents and the reconciling items to final disposition;

e) Review of a sample of incoming transfers for proper completion;

f) Determining if documentation exists on how rejected transactions were handled;

g) A review of messages to determine if they were delivered and accounted for;

h) A review of outgoing transfers to determine the propriety, proper authorization, and member accounts are properly charged;

i) Verification of outgoing wire transfers for accuracy to source document; and

j) A determination that the settlement of a transfer did not result in the members account being overdrawn.

Cell: B16

Comment: Best Practice: A log containing the information required per the Bank Secrecy Act Recordkeeping Requirement [31CFR103.33(E)(1)(i)] should be maintained.

Cell: B22

Comment: Credit unions should have member verification procedures in place for wire transfer requests. An example of member verification procedures for wire transfers requested in person would be use of photo ID. Credit unions which have a high volume of wire transfers, recurring member transfers, or accept phone requests should implement procedures to positively identify the requestor.

Cell: B23

Comment: Credit Unions should have a standard form requesting beneficiaries name, address, and purpose of wire. Member signatures should be required for all wire transfer requests.

Cell: B24

Comment: This is suggested in order to verify the accuracy of dollar amount of wires and the validity of the request. The credit union should perform a risk assessment to determine the maximum amount per policy. All exceptions to policy require management approval.

Cell: B25
Comment: Best practice - Credit union's should maintain recordings for 6-9 months but need to review state requirement in determining appropriate period for retention.

Cell: B35
Comment: Employees should receive training upon appointment to a position in the wire transfer department and thereafter receive annual training to reinforce the credit unions security and control policy.

Cell: B43
Comment: Verification procedures would vary based on the type of contact with members. For example, the procedures would be different for a member who physically visits the credit union versus one who contact the credit union via the telephone or other electronic means. The credit union should have written procedures and appropriate processes in place to authenticate members identity for each type of approved method members can contact the credit union to request a wire transfer.

Cell: B56
Comment: Best Practice - restricted access to wire area or PCs with wire transfer capabilities when possible.

Cell: B57
Comment: The report should provide management information on comparing actual activity generated by a specific employee and comparing the activity to the authorized limits of the employee, access levels, and separation of duties information.

Cell: B63
Comment: The periodic review performed should include at least the review of all insider accounts to detect any unusual "high dollar" or "frequent" wire transfers.

	A	B	C	E
3	**PAYMENT SYSTEMS -FRB**			
4	**INTRODUCTION AND PURPOSE**			
5	**EXTERNAL REFERENCES**			
6		**Connection:**	**Yes/No/NA**	**Comments**
7	1.0.0	Does the credit union use FedLine Advantage to access the Federal Reserve Bank (FRB)? If yes, document the method used to connect to the FRB in the comment section.		
8	1.1.0	Is the configuration of PCs with FedLine Advantage access:		
9	1.1.1	-Networked		
10	1.1.2	-Standalone PCs		
11	1.2.0	Has the credit union implemented the automatic failovers for the communication option chosen to access FedLine Advantage?		
12	1.3.0	Are the communication devices used to create a secure transmission of information located in a secured location?		
13	1.4.0	Are the devices attached to Uninterruptible Power Supply (UPS) surge protection equipment?		
14		**Administration**	**Yes/No/NA**	**Comments**
15	2.0.0	Has the credit union identified the employees who have key roles in the operation of FedLine Advantage?		
16	2.1.0	Does the list of PCs with the FedLine Advantage connectivity match the staff listed as authorized users?		
17	2.2.0	Do employee termination procedures take into consideration FedLine Advantage access and notification of the FRB?		
18	2.3.0	Is the terminated employee's FedLine Security Token retrieved immediately and properly disposed of by management?		
19	2.4.0	Is FedLine Advantage software access removed from the terminated employee's PC, if it will no longer be used for FedLine Advantage activities?		
20		**Physical Security**	**Yes/No/NA**	**Comments**
21	3.0.0	Are PCs authorized to access Feline Advantage placed so information or access cannot be easily observed?		
22	3.1.0	Are FedLine Security Tokens removed from PC's whenever the FedLine Advantage communications channel is not in use?		
23	3.2.0	Are there written procedures which address the secure storage of the FedLine Security tokens when not in use?		
24		**Security**	**Yes/No/NA**	**Comments**
25	4.0.0	Do PCs used at the credit union require an operating system user ID and password to logon to the PC?		
26	4.1.0	Is FedLine Advantage software only loaded on PCs of authorized users?		
27	4.2.0	Have PC(s) had their operating systems secured ("hardened") according to industry best practices?		
28	4.3.0	Are all PC(s) at the credit union included in the patch management program for:		
29	4.3.1	-Windows operating system(s)		
30	4.3.2	-Browser software; and		

	A	B	C	E
3	**PAYMENT SYSTEMS -FRB**			
31	4.3.3	-Personal firewall software (if applicable)		
32	4.4.0	Is personal firewall software installed on the PCs? (Note: If the PCs are contained in a network and the security is appropriate, personal firewalls do not have to be active).		
33	4.5.0	Is anti virus software installed and configured to be active on all PCs?		
34	4.6.0	Is the anti virus software program utilized by the credit union a current version which is supported by the vendor?		
35	4.7.0	Is a formal process in effect to update virus signature files and ensure that installed signatures are up to date?		
36	4.8.0	Is a full system virus scan performed at least once each week?		
37	4.9.0	Are PCs authorized to access FedLine Advantage included in the credit union's network security structure and sufficiently protected from external attacks?		
38	4.10.0	Is the security and functionality of the credit union's FRB access considered when contemplating/implementing changes to the network operating system, network infrastructure, network equipment configurations and settings?		
39		**Remote Access**	**Yes/No/NA**	**Comments**
40	5.0.0	Does the credit union prohibit remote access capabilities?		
41	5.1.0	Has the credit union identified and evaluated the risks associated with their remote access capabilities?		
42		**Documentation/Reports/Audit**	**Yes/No/NA**	**Comments**
43	6.0.0	Is FedLine Advantage documentation (printed and electronic) and the installation software CDs (FedLine Advantage Connection Utility and FedLine Security Token driver software) treated as confidential and accessed only by authorized personnel?		
44	6.1.0	Does the report secured from the software provided by the Federal Reserve accurately reflect the staff currently authorized and assigned access?		
45	6.2.0	Does the review of all reports generated from the software note any unusual activity?		
46	6.3.0	Has the credit union developed an internal or external audit program relative to the use of FedLine Advantage?		
47		**Incident Response**	**Yes/No/NA**	**Comments**
48	7.0.0	Does the credit union's incident response plan or procedures incorporate FedLine Advantage and address situations where the credit union is required to immediately notify the Federal Reserve Banks when:		
49	7.0.1	There is unauthorized disclosure of FedLine Advantage controls or documentation?		
50	7.0.2	There is unauthorized use of FedLine Advantage services?		
51	7.0.3	There is suspicion of fraud, tampering, infringement, or a security breach?		
52		**Business Continuity/Contingency Planning**	**Yes/No/NA**	**Comments**

	A	B	C	E
3	**PAYMENT SYSTEMS -FRB**			
53	8.0.0	Does the credit union have a documented and tested plan for utilizing FedLine Advantage in the event of equipment failure or a disaster situation?		
54		**Training and Awareness**	**Yes/No/NA**	**Comments**
55	9.0.0	Is there an on-going training and awareness program to train and update employees on their roles and responsibilities?		

Cell: B4

Comment: This questionnaire should be used to determine the adequacy and effectiveness of the security controls and business continuity planning for the credit union's implementation of FedLine Advantage for the funds transfer application. These procedures evaluate the effectiveness of the credit union's control environment and related risk management processes for the funds transfer application of FedLine Advantage.

The usage of these examination procedures should be based on the examiner's assessment of the risks and risk management practices related to the credit union's use of FedLine Advantage, including transaction volumes. This assessment should include consideration of formal policies and procedures, as well as an assessment of the effectiveness of the credit union's overall information security and business continuity planning.

Feline Advantage can be used for wires, ACH, share drafts, cash orders. Third party software is used to create batches transmitted through Redlined. Batches cannot be created in Feline Adv.

Cell: B5

Comment: Federal Reserve Board Operating Circulars OC-4, OC-5, and OC-6 which can be found on line at: http://www.frbservices.org/OperatingCirculars/index.html

Cell: B8

Comment: Networked - A group of two or more computer systems linked together.
Standalone PCs - Personal computers which are not connected to other computers or devices at the credit union.

Cell: B11

Comment: Two of the three FRB approved FedLine Advantage connection methods provide an alternative method to connect to the FRB in the event of a disruption. Credit unions should implement the failover option for the connection method chosen as discussed in FedLine Advantage Technical Support Liaison Guide provided by the FRB to ensure connectivity in the event of a disruption.

Cell: B15

Comment: The key roles are identified in the confidential booklet, FedLine Advantage Monitoring and Control Guidelines, provided by the FRB to the credit union.

Cell: B21

Comment: To prevent unauthorized information eavesdropping of PC(s), management should establish a level of physical security appropriate to its operating environment for the PC(s).

Cell: B22

Comment: The FedLine Advantage Security Tokens are contained on USB Memory Devices which are inserted into the USB Drives of the authorized Personal Computers at the credit union.

Cell: B26

Comment: No PCs should have the FedLine Advantage software installed unless they are designated for access to FedLine Advantage. Typically, credit unions move PCs among staff members when new computers are purchased. Sometimes the old software on the PC inappropriately moves with the PC to the new user of the PC. Check to ensure that this has not happened with Feline Advantage software.

Cell: B27

Comment: A key security practice is the removal of all unneeded operating system services (e.g. Internet Information Server (IIS) or other web servers, SQL server, peer-to-peer file sharing, SNMP, etc.). Best practices for securing Win2000 and WinXP operating systems can be found at www.nsa.gov and www.cisecurity.org.

Cell: B28

Comment: Many security patches are critical and it is very important that PCs have the latest security patches installed. The examiners should select a sample of one or two PCs and review the dates of the latest patches (normally should list patches within the last couple months) to verify that the credit union's patch management process is working.
To review:
• Start
• Settings
• Control Panel
• Add or Remove Programs
• Check "show upgrades" box at top
All patches are listed chronologically at the bottom (with install dates).
An examination exception should be cited if it appears the patch process in not in effect or not working correctly.

Cell: B32
Comment: Confirm that personal firewall software is active on each workstation/pc. For those workstations/paces running Windows XP (SP2), using the operating system's built-in firewall is acceptable. The software should be properly installed and configured, and regularly updated. Any alerting capability that is appropriate for the environment should also be enabled and monitored.

Cell: B34
Comment: Vendors periodically update the version of software which they supply to users for a variety of reasons. Credit unions normally need to be on the most recent version of the software to receive software support.

Cell: B37
Comment: Ensure that there are strong network access control mechanisms in place to protect the connection devices from unauthorized internal network access and external Internet access. More specifically:
• Use the network diagram and other relevant information to determine that the perimeter of the credit union's IT infrastructure is protected from external attack via an enterprise-wide or front-end firewall complex or equivalent system.
• Verify the credit union uses a network configuration where only PCs authorized to use FedLine Advantage can access the connection devices.

Cell: B40
Comment: Remote access is defined as the ability to log onto the credit unions network from a location outside the credit union facility(s). Generally, to access the credit union network remotely would require the remote user to have a computer, a modem or high speed internet connection, and some remote access software to connect to the network.

Cell: B41
Comment: To assist with the layered approach to security, ensure that there are reasonable security and controls in place (e.g., firewall and intrusion detection systems) to protect the organization's LAN/WAN network infrastructure from unauthorized access. Network access points such as the Internet, Extranet connections, wireless networks, and remote access solutions should be of special concern. Ensure that the risks to the FedLine Advantage system arising from any allowed remote access are satisfactorily identified and controlled. Similarly, where individuals that are granted Subscriber access are permitted remote access into the institution's network, ensure that risks to the system are appropriately identified and controlled. Verify that remote access was approved for each user by management/officials.

Cell: B43
Comment: Any documentation pertaining to FedLine Advantage is confidential and should be maintained in a secure environment and only utilized by authorized personnel.

Cell: B45
Comment: Unusual activity might include an unrecognized user removed before the exam, which does not correspond to a

valid terminated or transferred employee. The risk is that a credit union might assign two sets of credentials to one user for a single ABA number (thereby circumventing the dual controls between entry/update and verify) and then try to delete one set of credentials before the exam. Review the e-mail addresses of user on the system, credential, and service changes. All e-mail address should appear to be valid e-mail addresses tied to that particular employee.

Cell: B46
Comment: Although not required, it is recommended to perform an independent review of controls and procedures on an annual basis. Refer to Feline Advantage Monitoring and Control Guidelines for recommended audit procedures.

Cell: B48
Comment: If formal incident response plan does not exist, these requirements may be listed in a wire transfer policy or security policy.

Cell: B49
Comment: Per OC-5, the Certification Practice Statement and the Password Practice Statement.

Cell: B50
Comment: Per OC-5, the Certification Practice Statement and the Password Practice Statement.

Cell: B51
Comment: Per OC-5, the Certification Practice Statement and the Password Practice Statement.