

WIRE TRANSFER GUIDE

WIRE TRANSFER METHOD:

	1	Fedline Advantage/Fedline Web from Federal Reserve Bank
	2	Autosolution from Bankers' Bank
	3	Telephone
	4	Other (Internet)

COMPUTER SETTINGS - FEDLINE ADVANTAGE/FEDLINE WEB

Obtain the Users' lists and print screens of Processing Options - Settings and Processing Options - Verification. This information can be obtained by the bank.

<p>There are four different roles relating to Fedline wiretransfers. The End User Authorization Contact (EUAC) is the main contact with the FRB. A bank should have at least two EUACs. They are the individuals who designate the individuals at the bank who will perform wires. The EUAC can reset passwords and access subscriber reports and Fedline documentation. The Supervisor updates processing options (settings, verifications, and e-mail notifications) and CANNOT create, import, update, or verify wires. Appears should also have at least two Supervisors. The Transfer Specialists are the bank employees who create, verify, view, and print the wire transfers. The analysts can only view and print wire transfer data, therefore have a limited role in the wire transfer process.</p>	1	<p>Are the user lists (of the Transfer Specialists, EUAC, and Supervisor) accurate?</p>
<p>Examiners will recommend that employees not have dual roles in the categories set up through Fedline. Because in many small banks the security officer is often involved in wire activity, we will use common sense when dealing with this matter; however, examiners should ensure that security controls detailed within this section are properly set to compensate for the Funds Supervisor being involved in the wire transfer process. Some institutions may have three employees with security authority in case a backup is needed. While this is not the preferred method, it is acceptable.</p>	2	<p>Are the bank employees who have been given EUAC, Funds Supervisor, and Transfer Specialist assignments mutually exclusive, with an appropriate number of individuals in the EUAC and Funds Supervisor roles?</p>

	3	Are Processing Options - Settings set so that duplicate reference numbers are not allowed?
While this may be a high number, the EUAC should have determined what the highest wire transfer amount will be and complete this box accordingly. Examiners should note if the number appears excessive.	4	Has a "Maximum for message amount" been established on the Processing Options - Settings page?
This is the strongest, and therefore the recommended setting, as selection of this option requires the dollar amount of the wire to be reentered. Sight verification calls for a review of the wire transfer with no rekeying of information. The None selection is not recommended.	5	Does Processing Options - Verification call for Key: \$Amount verifications?
Selection of one of these two options requires that at least two individuals must be involved for each wire transfer. The selection of the option that Verifier can be the same as Enterer and Updater(s) is not recommended.	6	Does Processing Options - Verification require verifier either "must be different from Enterer and Last Updater" or "must be different from Last Updater?"
Verification should ideally be set at 0.00 meaning all wires require verification; however, some banks may set at a higher amount, such as 1,000. The higher the verification amount the greater the risk to the financial institution. If the amount is large it should be approved by the board of directors. I have not been able to find out if no number (blank) is the same as 0.00 or not. For safety purposes, request the bank put in 0.00 if that is what was intended.	7	Is the "Verify value messages over and including" box under Processing Options - Verification set at 0.00 or a reasonable amount?
	8	What security is in place for tokens during banking and non-banking hours?

COMPUTER SETTINGS - AUTOSOLUTION

The printout needed for a review of Autosolution would be the Security Profile Report. This report will show all of the users and their security levels. The last page will show the program timeout. To access this report, an employee with the report function checked would go to the Application button in the main menu, create the report, and then go to Report Manager and print the report.

<p>The types of wires available are noted as EXP (Expanded), IN (International), and IMP. Wires that are over 3M automatically require the name and address of the sender to comply with BSA.</p>	
<p>Other than program timeout, the security controls are pre-set at satisfactory levels and can only be made tighter by the bank; therefore we will not need to check most information other than the program timeout. The program timeout is recommended to be not more than 20 minutes (10 is the ideal) but can be set for up to 60 minutes. If examiners want a copy of this information it can be print-screened.</p>	
<p>Examiners want to make sure that personnel who no longer perform wire transfers or are no longer employed by the bank are not on the list. A bank has to pay a fee to Bankers' Bank for each person on the list, so they likely will want to have as few authorized people as possible on the system.</p>	<p>1 Does the Security Report accurately reflect the individuals who are needed to perform wire transfers?</p>
<p>This is the only security information that can be changed by the bank.</p>	<p>2 Is the Program Timeout set to 20 minutes or less?</p>
<p>Examiners will recommend that the individuals with security authority (denoted by Modify Security authority on the Security Report) not be able to perform funds transfers. The security officers are also the only individuals who should have the edit environment authority checked. With this new Autosolution program, NO employees are permitted to verify their own wires. Because in many small banks the security officer often is involved in the wire activity, we will use commonsense when dealing with this matter. Encourage them to make a change if feasible, but the second verification negates some of the concerns. We will want the bank to have a more thorough review of the available reports by an uninvolved party.</p> <p>Some institutions have three employees with security authority in case a backup is needed. While this is not the preferred method, it is acceptable.</p>	<p>3 Have a limited number of individuals (preferably not more than three) been given security authority, and are these employees prohibited from performing funds transfers?</p>

TELEPHONE TRANSFERS

<p>The bank should have a customer setup form from its correspondent bank. They may or may not have further agreements, as if they use a telephone system they probably don't have a lot of wire transfer activity. We would look for password controls for authorized employees, callback thresholds (some banks choose not to have this, which is not a good idea), and who is authorized to process requests on behalf of the bank.</p>	<p>1 Are current funds transfer agreements in effect between the institution and its correspondent bank?</p>
<p>We recommend that the callback threshold be zero. This may not be feasible for some large banks, but it should be as low as possible. <u>The Board of Directors should approve any amounts above zero.</u></p>	<p>2 Are callbacks required from the correspondent to subject bank for outgoing wire transfer amounts?</p>
<p>Examiners should look for some form of immediate verification if there is not a callback. The correspondent bank will likely send a fax verifying the request. In some banks this will likely be followed by a hard copy advice sent through the mail. The information would also be contained in the bank statement, although it may be an extended period of time before the bank receives this.</p>	<p>3 Is there a method for verifying outgoing requests made by the bank, particularly if a callback is not used?</p>
<p>We need to ensure is that an employee has a private place to go to call in or verify a wire request if they have to verbally give their password over the phone. Again, authorized employees should keep passwords confidential and there should be no shared passwords. Passwords should not be written down and left in a desk drawer so all employees have access to them. Be sure to ask open-ended questions and you might be surprised at the answers as to whether or not passwords are kept secure.</p>	<p>4 Is there a private place for employees to execute the transaction?</p>

The bank wants to ensure that there is actually an incoming wire. If only verbal notification is made, the bank should call back to their correspondent and ask for confirmation.	5 When telephone advises of incoming transfers are received, do employees assure themselves that the person initiating the call is authorized to do so?
---	---

OTHER

At this point it is not possible to develop specific questions for the less common wire transfer programs certain banks may be utilizing. If an Internet based system with preset security levels, examiners can follow the Autosolution questions. For other computer-based programs, examiners can ask the following questions. Keep in mind that the most important thing is to ascertain suitable security settings are in place, the system is monitored, and appropriate personnel are allowed to utilize the system.

	1 Does the bank maintain an accurate list of authorized users?
	2 Have no more than two individuals been given security authority and are these individuals restricted from funds transfer and send applications?
	3 Will the user be kicked off the system after three or fewer failed log in attempts?
	4 Will the system automatically log-off after not more than 20 minutes of inactivity?
	5 Are users required to change their password every 30 days or less?
	6 Are users prohibited from verifying their own wire transfers?
	7 Do authorized individuals have only one User ID each?
	8 Have users been restricted to only necessary applications?
	9 Does management print and review an activity report on a daily basis?

POLICIES AND PROCEDURES

<p>Examiners are going to strongly recommend that banks have written procedures, regardless of the amount of wire transfer activity, in order to provide the necessary direction and support to the banking staff. We want the bank to document who can do transfers, how they will do it, and what safety and security measures will be implemented.</p> <p>Because of the controls built into Fedline and Autosolution, the absence of a policy is not always a major concern.</p>	<p>1 Has the bank formulated written wire transfer procedures or a wire transfer policy that addresses:</p>
	<p>a. The method that the bank will use to complete wire transfers?</p>
<p>List specific employees authorized to take the wire transfer request or originate the actual transfer. In larger banks this may be by classes of categories, such as tellers, etc. Identify employees who perform wire transfer activities such as wiring funds, verifying wire instructions, and performing call backs. The BOD should review and approve this list annually.</p>	<p>b. Authorized users for the initiation and verification of wire transfers?</p>
<p>This amount can be whatever the Board determines is satisfactory. Our recommendation is that the verification threshold be zero, although this may not be feasible for some large banks. The Board would need to determine their “tolerance for pain” if they want to establish a higher threshold.</p>	<p>c. Dollar amount thresholds for initiation and verification (callback)?</p>
	<p>d. Appropriate documentation?</p>
	<p>e. Security controls applicable to the method the bank has chosen to use (particularly if the bank uses the telephone)?</p>
	<p>f. Terminal security and password control?</p>
	<p>g. Supervisory review of activity?</p>
	<p>h. Maintenance of wire transfer agreements for customers?</p>

See #2 under Customer Records.	i. Customer verification procedures?
	j. Maintenance of a wire log?
	2 Is the bank in compliance with written procedures/policies?
<p>Officers should perform internal reviews to detect possible circumvention of established internal controls and system security measures. What we want to ensure is that there is sufficient control over the wire transfer activity. The depth of the review would vary given the level of activity and the "threshold of pain" that the Board has established. It doesn't hurt to remind management that it won't cost them anything to put thresholds in place, and it may save them money in the long run. In some instances the Board may rely on CPA examinations for this review, although I have not noticed many instances where the examination has discussed wire transfer activity. Per the FDIC, this is okay unless there is a large volume of activity or if there are problems. If concerns exist, we should tell management that it would behoove them to do regular reviews.</p>	3 Does management perform periodic internal audits/reviews to ensure compliance with wire transfer policies/procedures and recommended guidelines?
	4 To the extent possible, are the receipt, processing, authorizing, accounting, and reconciliation functions adequately segregated?
<p>There should generally be a separation between the authority to initiate wire transfers and the authority to approve said transfers. An exception to this might be FFS or participations. Ask who can initiate and approve wire requests – make sure the same person cannot do both on the same request. This has to do with segregation of duties. At some banks the individual who takes and/or prepares the request is different from those who originate the actual transfer, therefore this list may or may not be different from the various user screens or the telephone transfer set-up sheet. It should be reviewed by the Board.</p>	5 Is a current list of bank personnel authorized to take requests and initiate wire transfers maintained and is this list reviewed annually by management?

<p>It should be documented if established authority limits have been exceeded, or special authorization procedures should be in place and noted for transfers in excess of prescribed employee limits.</p>	<p>6 Have dollar limits been established for these employees?</p>
<p>In general, wire transfers should be a service performed for customers of the institution, not individuals who walk in off the street. Non-customer wire transfers should be made for cash only (that is, checks, money orders, or cashiers checks should not be accepted). Typically, I have seen that if this is done, the cash is “deposited” into a specially designated account, and then this account is referenced as the wire transfer is performed.</p>	<p>7 Does the bank restrict or prohibit wire transfers for non-customers?</p>
<p>Examiners should follow-up on deficiencies noted and ensure that suggestions for improvement have been implemented.</p>	<p>8 If any deficiencies have been noted by regulators, auditors, or as the result of internal audits, have they been corrected?</p>

CUSTOMER RECORDS

<p>It is recommended that wire transfer requests be made in person and signed unless a wire transfer agreement is in place.</p>	<p>1 Is written authorization obtained from customers for outgoing transfers before the transfer takes place? (This is especially important for new large dollar wire transfers)</p>
<p>It is strongly recommended that requests are required to be made in person for the protection of both the customer and the bank. If practices allow outgoing wire requests via telephone or fax, identification procedures should be in place to ensure an authorized individual is performing the request. There should be documentation that can be maintained to detail how the customer was verified. If verification is not done by passwords, it could use such information as the date and amount of last deposit, etc. SS or Tax ID numbers should not be used. Some banks tape the requests, but this is not realistic for our small community banks. A signed copy of the fax should be received to verify the signature of the requesting individual. A callback to the number on file for the customer is also a possibility.</p>	<p>2 If the institution allows for outgoing wire requests via telephone or fax, has the bank established guidelines for using a callback procedure, to the number on file for the customer, to verify the authenticity of the requests?</p>

<p>The best method would be for banks who are not requiring requests be made in person to obtain written authorization and signatures from customers before wiring funds rather than relying on voice recognition and/or call back procedures.</p> <p>Many banks do not implement callbacks unless wire transfer is above a certain amount. Always encourage them to implement dollar volume thresholds (as low as possible and preferably zero) and callback procedures.</p>	
<p>Wire transfer agreements should be treated as confidential information, especially if customer passwords are contained on this forms that are used for verifying/authenticating telephone requests. These agreements should be treated similarly to any other confidential information in the bank. The wire transfer request is generally prepared by the employee(s) with access to the agreement so they can check test keys and passwords. Ideally, the person who enters wire transfer information (either over the phone or through a computer program) should not have access to these agreements.</p> <p>The written agreements should inform customers that passwords are to be kept confidential.</p>	<p>3 Does the bank have written agreements and authenticating controls (test keys and/or passwords) with each of its business customers who use wire transfer services on a regular basis?</p>
	<p>4 Do these agreements authorize individuals who can request wire transfers and set dollar limits for each of these individuals?</p>
	<p>5 Are written requests verified against the authorized signature list?</p>
<p>The customer should be required to promptly notify the bank of any personnel changes. This is an extremely important topic that needs to be addressed in the agreement. Many banks renew business wire transfer agreements on an annual basis.</p>	<p>6 Are customer agreements periodically reviewed and updated to ensure that authorized individuals have not changed?</p>
<p>The person who responds to the callback to the business must be different from the initiator.</p>	<p>7 Have callback requirements been implemented?</p>

<p>The bank employee who takes the request can also do the callback to the business, although it would be an additional security measure if a second person at the bank did the callback.</p>		
<p>Unauthorized loans may result if transfers are completed with uncollected funds. The bank should have an acceptable accounting/computer system in place to prevent this from happening. We may want to ask if the computer system can differentiate between collected and uncollected deposit balances.</p>	8	<p>Are procedures in place to check for collected funds in deposit accounts or preauthorized credit availability prior to the sending of wire transfers?</p>
	9	<p>If the bank does allow transfers against uncollected funds, is the excess amount approved by an officer who has the appropriate credit approval authority?</p>
<p>If a customer wants to pay cash for a wire transfer, the amount should be verified and then the customer should be escorted to the teller line for deposit of funds.</p>	10	<p>Has the bank developed satisfactory procedures to handle cash transactions?</p>
<p>Ideally employees should have limited access to this information, as it is confidential and should be treated as such.</p>	11	<p>Is access to test keys, password, and customer wire transfer agreements properly controlled?</p>

RECORDKEEPING

<p>Keep in mind that some banks may not complete incoming forms if they use an automated program like Autosolution, since the information can be printed off.</p> <p>Some banks may have a dollar limit for the recording of forms. We will recommend that all wire transfers be recorded on a form. Keep in mind that at some institutions they also keep a wire transfer log that lists all wire transfer activity. This log may only include those transfers above a certain amount.</p>	1	<p>Has the bank developed a form, or implemented procedures, that allow for the capture of the following required wire transfer information at origination:</p>
---	---	---

The bank may have just one standard form. Some may not have a form and instead just put the information on a blank piece of paper.

EXAMINERS WILL RECOMMEND THAT THEY ALWAYS USE A STANDARDIZED FORM.

In some instances the details may be pretty sketchy, particularly for participation payments, but employees should always get any necessary approvals.

To ensure sound practices, dual control should be used and the requests should be signed by the preparer and a reviewer. If a customer makes the request in person, would we always want them to sign the bank's wire transfer form. Several banks instead have the customer sign the cash withdrawal form, we will recommend that the customer signs both.

This would include the signature of the customer, whom hopefully is required to make the request in person. In some instances the customer may sign the withdrawal ticket. While it is preferable that they also sign the request form, a copy of the signed withdrawal ticket attached to the form is acceptable.

a. Name and address of the originator?

b. Details of ID used to verify identity of the originator (unless is an established customer and the bank has already recorded name, address, and TIN)?

c. Account number of the originator, if payment was ordered from an account?

d. Amount of the payment order?

e. Any payment instructions?

f. Identify of the beneficiary's bank?

g. The beneficiary's name, address, account number, and any other specific identifying information as are received with the payment order?

h. Space for the appropriate signatures of the customer, initiating employee, and a reviewer?

i. A place to note if the customer's deposit account was reviewed for collected funds or preauthorized credit?

	j. A place to note if the OFAC list was checked?
For BSA records, the minimum retention period is five years, with the FDIC recommendation being seven years. All audit trail information (the log book form for customer authorization as well as any summary reports) should also be retained for at least five years.	2 Are bank records for wire transfers retained for the appropriate time period?

COMPUTER SECURITY

<p>A segregated wire transfer area is usually only for large wire transfer operations. Most of the community banks in Iowa should have appropriate controls given the size and complexity of the department and how the transfers are generated. If the transfers are generated via a software package (Fedline or Autosolution) the controls are going to be security access, password controls, and terminal controls. If wires are requested through a third party (UMB, Wells Fargo, etc.) then there should be appropriate controls over passwords and callback procedures.</p> <p>Confidentiality of passwords, test keys, agreements, and proper authorization of the transactions is the key – not necessarily control over the entire environment.</p>	1 To the extent possible, is physical access to the wire transfer equipment and codes limited to authorized personnel?
---	--

WKSht - WireTransGuide (Rev 12/31/07)