



Best Practices for Bank Account Entry and Assignment

Overview

Vendors that are paid via ACH have their bank account information entered at the Supplier Site level in order for the ACH program to send this information to the bank. The set up of bank accounts in Oracle is a prerequisite to the assignment of that bank account to a Supplier. Employees that have access to the bank accounts form can set up a bank and related bank account, then can also assign that bank account to an existing supplier. An employee that knows of a supplier that is paid via ACH could set up a fictitious bank account, and then assign it to that supplier in the bank accounts form, causing a company to pay the fictitious bank account.

Control Objective

The objective of this control is to provide for the entry of bank account information for the set up of a supplier so they can be paid via ACH, but for a secondary review (either manually or programmatically) once the initial data entry is done. This review is primarily to prevent the ability of a person (barring collusion) to commit fraud.

Scope

The scope of this document is the best practices related to bank account entry and monitoring of such once a company has an approved form that contains the bank account related information for a Supplier. See related document Supplier Form Personalization related to Supplier bank account information that covers the hiding of such restricting view access from such sensitive data once it is assigned to a Supplier. See further definition of scope in the caveats section at bottom. The scope of this document does NOT include bank account management related to payroll/HR data.

What can be done about it?

There are two underlying issues that need to be addressed. First, it is important to discuss the role of the person who has the ability to maintain the bank account information. Second, it is necessary to provide a review of such data entry to. Both will be discussed in more detail.

Who should do bank account entry and maintenance?

Perhaps the most important question is who SHOULDN'T be the person having access to the bank accounts form. A company needs to determine how and when it is appropriate for accepting requests to set up a supplier for payments via ACH. This process is outside

of the scope of this document. The starting point of this discussion is that an employee has a form or email that an approval has been given to them to set up a supplier for ACH payments using Oracle Payables. Since this bank account information can be assigned also at the Supplier Site level, it is critical that the person who has access to the Suppliers form, to maintain this field should NOT be allowed to maintain information in the Bank Accounts form. Allowing a person to do so would allow them to create a fictitious bank account and assign to a supplier that is paid via ACH, thus defrauding a company. Typically, since this setup has the effect of determining how a Supplier is paid, the person doing this maintenance should also NOT be involved in any other Supply Chain process such as initiating requisitions, issuing purchases orders, issuing payments or entering invoices. The process of entering bank account information should be viewed as merely a clerical function based on an approved form/email and could be performed by anyone outside these processes mentioned.

How should a review of such data entry be done?

Bank Account information and the related processes are typically included in Key Controls. Therefore, it is important and necessary that company's identify a method to validate that the data entry is appropriate, complete, timely and accurate. Two solutions are offered for consideration.

Option 1: A company could develop a custom workflow process that would force a secondary approval of the data entry of changes to the information. The workflow would be triggered on the data entry into the bank accounts form and the first person would enter the data based on the form provided by the employee or supplier. The form would then be passed to the approver (who should only be given inquiry access to the bank accounts form), where a second person would verify that the data entry was accurate and then approve the workflow notification. This would provide for a preventive control and would be better than a detective control.

Option 2: A company could have a manual control on this process where the information entered could be reported on and reviewed by a second person that would compare it to the approved form. However, out of the box, the applications don't provide an adequate audit trail for such a report. The standard audit trail provided is the Created By, Last Updated By at the record level. For complete detail on what was changed, an advanced audit trail is necessary. This audit trail needs to be created by enabling audit from the System Administrator responsibility by setting the profile option "AuditTrail:Activate" to 'Yes' and then enabling such an audit for the following tables: Bank Accounts - AP_BANK_ACCOUNTS_ALL, Bank Branches - AP_BANK_BRANCHES, and Bank Account Uses - AP_BANK_ACCOUNT_USES_ALL. When using the standard 'advanced' audit trail functionality, the system creates a trigger that throws the field level change to shadow tables (for example, AP_BANK_BRANCHES_A). Your next challenge will be to report on this information. Reporting could be done via an RDF, Discoverer, or some other medium. Another option for you in the creation of an advanced audit trail would be the purchase of a third party tool which several companies offer to help facilitate the enabling and reporting of such information (contact the author for a list of these companies).

Other options that have been suggested:

1. Perform a test transaction against such supplier with a \$0 invoice and view the output file.
2. Develop a custom trigger to notify someone of the data being entered/changed.
3. Use Alerts to notify a reviewer/approver of additions/changes to bank account information.

What other issues are there?

The final piece to this puzzle is to prevent the person that maintains the bank account from also assigning the bank account to the supplier. As mentioned above, the person performing maintenance on the bank account should not be able to maintain the supplier master information. However, the bank account form also allows the assignment of a bank to a supplier. The Supplier Assignment tab (see below) should be removed/hidden via *forms personalization* (or other tool that writes into the custom.pll) so that the responsibility related to bank account maintenance cannot maintain this field.

The screenshot shows the SAP 'Banks (Vision Operations: USD)' form. The 'Bank Accounts' section is expanded, showing fields for Bank Name (010), Branch Name (213), Operating Unit (Vision Operations), Agency Location Code, Name (Test Supplier Bank), Alternate Name, Account Use (Supplier), Account Type, Number (12345), IBAN, Currency (USD), Inactive On, Description, and Check Digits. There is a checkbox for 'Allow Assignment to Multiple Suppliers'. Below this is a tabbed interface with 'Supplier Assign...' selected. The 'Supplier' table shows one entry: 'Fraudulent Supplier' with Number 20027, Site FRAUD, and Effective Dates from 14-JUL-2006. The 'Primary' checkbox is checked. At the bottom, there are buttons for 'Payables Documents' and 'Bank Codes'. The status bar at the very bottom shows 'Record: 1/1' and '<OSC>'.

Once this is assigned to a Supplier Site, it is visible in the Suppliers form as follows:

Supplier Sites (Vision Operations: USD) - Fraudulent Supplier, 20027

Site Name: FRAUD
 Country: United States
 Address: 12345 Fraudulent Lane
 City: Fraudville, State: CA, Postal Code: 92453

Name	Number	Curr	Primary	Effective Dates
				From To
Test Supplier Bank	12345	USD	<input checked="" type="checkbox"/>	14-JUL-2006
			<input type="checkbox"/>	
			<input type="checkbox"/>	

Bank Name: 010
 Branch Name: 213

Record: 1/1 | ... | List of Valu... | <OSC>

Employee bank data and data sensitivity implications

If you have employees set up as suppliers and also have their bank account entered so they can receive payments from AP via ACH, there are additional considerations. Many states have laws that require the securing of employee data such as home address and bank account information (not all state laws have the same requirements). In addition, with identity theft on the rise, regardless of what statutes with which you are required to comply, it is a good business practice to limit the visibility to this information as much as possible. However, contradicting this is the fact that many people need inquiry access to the supplier master to see various data related to the suppliers. This typically includes the purchasing and accounts payable departments. Allowing full access for all employees to this data is not prudent. There are two primary methods by which this data could be protected. The first method would be to encrypt the data at the database level. This is the most secure method because the encrypted data cannot be viewed by anyone via the forms. However, it makes the validation process discussed above more difficult because the approver or reviewer needs to see the underlying data. A second method would be to use forms personalization or writing code into the custom library (see comments above) to remove visibility to this information. You can do this by applying the rule to the responsibilities that have inquiry access, but allowing the responsibilities that need to maintain or approve it to see such information. The full scope of this rule will be addressed in another white paper, but needs to include visibility to such information in the bank account form, supplier and supplier sites forms, and the invoice workbench.

Recognize also that the bank information is visible in several standard reports. See list of sensitive data and related standard reports by signing up for the Oracle Internal Controls

Repository at: <http://groups.yahoo.com/group/oracleappsinternalcontrols/>. This information is available in the Files section under the Internal Controls Content folder in a file called 'Reports with access to sensitive data.xls.'

Seeded functions provided by Oracle

The following functions have been provided by Oracle in newer releases of 11.5.10 (see Metalink Note 376058.1): Bank Account Access: Supplier, Bank Account Access: Customer, Bank Account Access: Internal, Bank Account Access: Supplier Assignments. The first three help distinguish what banks (Internal, Supplier, or Customer) can be access through this form and will help your differentiate the access to this data where it is necessary to do so. The fourth Bank Account Access: Supplier Assignments removes the ability for a user to assign a bank to an existing supplier. If these functions are available in the version you are running, please test them to make sure they are working properly. There was a bug Oracle noted (internal bug 685350) at one point. The control issues surrounding this are too critical to have issues with them because of an Oracle bug.

Segregation of Duties issues

The bank account entry function and the supplier master maintenance functions should be separated to avoid allowing the same person to create a fictitious bank to assign to a fictitious supplier. From a process flow perspective, here is an ideal scenario:

1. A person receives a request to set up a supplier bank account (either via email or via a form). That person enters the bank account information in the banks and bank accounts forms, but is unable to assign it to a supplier.
2. A second person reviews or approves the data entry, but is unable to update the information. The verification is done versus the request (email/form) from the actual requestor.
3. A third person (or could be the same person that is doing the verification of data entry) assigns the bank account information to the supplier via the supplier sites form.

Caveats

This white paper does not take into account the following:

1. Issues of viewing, inserting, or updating existing records at the database level. Database access controls are outside the scope of this document.
2. Mitigating or compensating controls that are not mentioned in this paper.
3. The possibility of collusion between two or more parties.

You should also recognize the importance of discussing any controls you design and implement with your company's senior management, including your signing officers, and legal representation as well as your external auditors.

Comments and feedback regarding this paper should be addressed to the author at jhare@erpseminars.com or by completing and forwarding a reviewer feedback form that can be downloaded at <http://oubpb.com/OUBPBWPRviewerFeedback.pdf>.

About the Author

Jeffrey T. Hare, CPA is one of the world's leading experts on the development of internal controls in an Oracle Applications environment. Jeff founded ERP Seminars and the Oracle Users Best Practices Board and is leading the efforts for the development of a public domain internal controls repository. See a full bio for Jeff at <http://www.erpseminars.com/providers.html>.

Version Control

Version	Updated by	Date	Comments
1.0	Jeff Hare	23-Aug	Initial release to IC Repository group and for public review
1.1	Jeff Hare	24-Aug	Added alerts to other options
1.2	Jeff Hare	24-Aug	Updated scope to exclude HR/PR bank account/direct deposit data
1.3	Jeff Hare	28-Aug	Change for file relating to reports with sensitive data
1.4	Jeff Hare	25-Sep	Updated for peer review comments