OFS Price Creation and Discovery Cloud Service

Service Access Control Guide

Release 9.0

October 2019

ORACLE
FINANCIAL SERVICES

ORACLE

OFS Price Creation and Discovery Cloud Service

Document Control

Version Number	Revision Date	Change Log
9.0	30 October 2019	First release

Table of Contents

1 Preface

Oracle Financial Services Price Creation and Discovery (OFS PCD) Service Access Control user guide explains the step-by-step instructions for controling the access for different user types and user groups.

This chapter discusses the following topics:

1.1 Audience

The target audience to this guide is the different roles within the bank that are involved in setting up/ configuring of the product and daily users. It is targeted towards the Administrators, Analysts, Implementation partners, Relationship Managers & Product Managers.

1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1.3 Related Documents

This section identifies additional documents related to Pricing Management Application. You can access Oracle documentation online from OTN:

Price Creation and Discovery Configuration and Installation Guide.

1.4 Conventions

The following text conventions are used in this document:

Conventions	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

Conventions	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1.5 Acronyms

The following acronyms are used in this document:

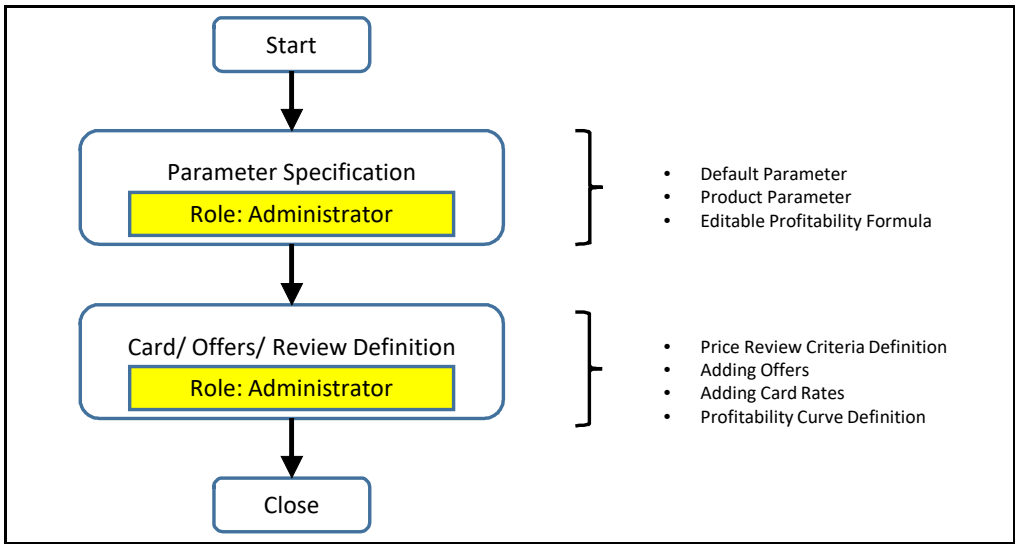
Acronym	Description
TP	Transfer Pricing
Expenses/ Cost	Total value of indirect costs like loan servicing costs, employee salaries that is allocated to a product
Fee Income	Income generated by a product based on the fees charged
NII	Net Interest Income
RAPM	Risk Adjusted Performance Measures
RAROC	Risk Adjusted Return on Capital
NIM	Net Interest Margin
ROTA	Return on Total Assets
SVA	Shareholder Value Added
UL	Unexpected Loss
EL	Expected Loss
FTP	Fund Transfer Pricing

2 Application Security

This chapter discusses the following topics:

2.1 Business Process Flow

The business process flow for the service security is shown below:



The process flow is described below:

- You need to specify the parameters before starting the process. This product will support three key methodologies:
  - Carded: In this method, the interest rate is pre-set and fixed by the banks.
  - Negotiated: In this method, the interest rate is negotiated with the customer.
  - User Input: In this method, the banks can input their own rate of interest based on certain parameters.

A Carded process involves finding a suitable price for the customer based on a pre-determined (set of) options available for that product and other dimensional combinations.

A Negotiated process allows the banker to determine a suitable price points within a set of thresholds determined by the bank/banker in order to solve for a target profitability parameter.

2.2 User Roles and Actions

The actions for the respective users are:

- **Bank Administrator**: The bank administrator has the following roles:
  - Setting up Parameters
  - Price Review

- Adding Card Rates

- **Relationship Manager**: The product pricing process begins with the analysis of the type of customer. The Relationship Manager analyzes and identifies whether the pricing is for an existing customer or a prospective customer.

  a. In case of existing customers, gather the relevant customer details from the system.

  b. The relationship manager also specifies the details of the product to be priced and the details of the deal including the methodology of pricing and other relevant parameters.

  c. Once sufficient information has been gathered about the customer and the product, the relationship manager would use the Price Creation and Discovery application to derive the final rate for the customer.

- **System Administrator**: A System Administrator creates roles and maps users. Access is provided to a user at the top of the hierarchy. Access is defined in terms of product and geography hierarchy. Users created by system administrators follow similar hierarchy with restricted access.

- **Credit Analyst**: The credit analyst has the following roles:

  - Adding card rates
  - Adding offer rates
  - Creating price review definition

2.3 User Access

The following tables explain the tasks that can be performed by various users in the Price Creation and Discovery application.

Role	Deal Pricing	Description
Relationship Manager	Yes	A Relationship manager has limited access; only to those account/customers that he is mapped to.
Pricing or Business Analyst	Yes	
Credit Analyst	Yes	
Admin or Super User	Yes	
Product Analyst	Yes	

Role	Card Rate Definition	Description
Relationship Manager	No	
Pricing or Business Analyst	Yes	View Only
Credit Analyst	Yes	View and Edit
Admin or Super User	Yes	Create and Edit

Role	Card Rate Definition	Description
Product Analyst	Yes	Create and Edit

Role	Offered Rate Definition	Description
Relationship Manager	No	
Pricing or Business Analyst	Yes	View Only
Credit Analyst	Yes	View and Edit
Admin or Super User	Yes	Create and Edit
Product Analyst	Yes	Create and Edit

Role	Accounts Flagged for Review	Description
Relationship Manager	Yes	
Pricing or Business Analyst	Yes	View Only
Credit Analyst	Yes	View and Edit
Admin or Super User	Yes	Create and Edit
Product Analyst	Yes	Create and Edit

Role	Account Review Criteria Definition	Description
Relationship Manager	No	
Pricing or Business Analyst	Yes	View Only
Credit Analyst	Yes	View Only
Admin or Super User	Yes	Create and Edit
Product Analyst	Yes	View and Edit

Role	Editable Profitability Formula	Description
Relationship Manager	No	
Pricing or Business Analyst	Yes	View Only
Credit Analyst	Yes	View Only
Admin or Super User	Yes	View and Edit
Product Analyst	Yes	View Only

Role	Profitability Curve Definition	Description
Relationship Manager	No	
Pricing or Business Analyst	Yes	View Only
Credit Analyst	Yes	View Only
Admin or Super User	Yes	View and Edit
Product Analyst	Yes	View Only

3 Data Security

The following The following table explains the applications roles which can see the PII information with/without redaction.

Application Role	Description	PII Visibility
UGPRMGRADMIN	PRMGR Application Administrator	Yes
UGPRMGRANALYST	PRMGR Application Analyst	Yes
UGPRMGRAUDITOR	PRMGR Application Auditor	Yes
UGPRMGRBANLYST	PRMGR Business Analyst	Yes
UGPRMGRCANLYST	PRMGR Credit Analyst	Yes
UGPRMGRINBOXADMIN	PRMGR Inbox Administrator	No
UGPRMGRPANLYST	PRMGR Product Analyst	Yes
UGPRMGRRM	PRMGR Relationship Manager	Yes

Additionally, the following user groups are introduced for GDPR compliance:

- Data Controller: This group has the privileges to maintain the PII list and Redaction policies against them. This group also has the privileges to ensure the Right to be Forgotten.
- Data Security Group: This group has the privileges to see the PII in un-redacted manner when the reports are access through OBIEE.

3.1 Right to be Forgotten

Right to be Forgotten is the task of removing PII (Personally Identifiable Information) of a Data Subject for the given Party. The financial institution can delete PII for those Data Subjects who have requested this Right to be Forgotten functionality.

The Data Subjects may have made significant financial transactions, and/or financial information may be required for regulatory or compliance reporting. Deleting the complete record that consists of PII may lead to issues in data reconciliation. In OFSAA, the PII data will be replaced with randomized values and therefore, the complete Data Subject record is retained. As a result, financial information is retained; however, the associated Party PII is removed permanently.

This section covers the following sub-sections:

3.1.1 Implementation of Right to be Forgotten by OFSAA

To implement Right to be Forgotten:

1. Use the FSI_PARTY_RIGHT_TO_FORGET table to collect the input list of Party IDs for which PII must be removed from the system. The financial institution must source this Party ID list into

the FSI_PARTY_RIGHT_TO_FORGET table, and then invoke the batch (<<INFODOM>>_RightToForget) or schedule it.

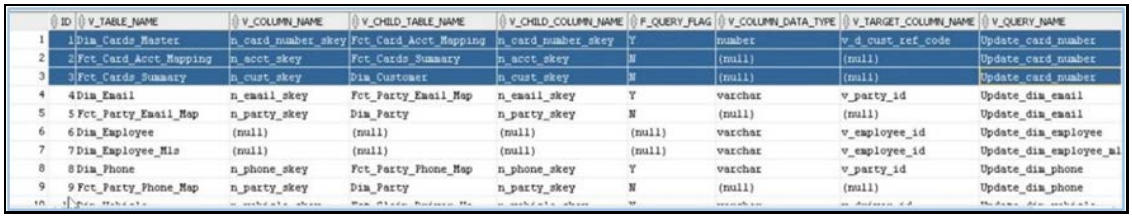
> **NOTE** For sample query, see Sample Query for the FSI_PARTY_RIGHT_TO_FORGET table.

2. Use the AAI table AAI_DRF_FUNCTION_COLUMN_MAP to store the PII attribute list. During the Right to Forget batch execution, AAI_DRF_FUNCTION_COLUMN_MAP table is referred to randomize the PII values. See the Data Redaction section in OFSAAI Administration Guide.
3. Use the AAI table AAI_DRF_QUERY_METADATA to store the query metadata, which is used during the <<INFODOM>>_RightToForget batch execution. This is the query metadata table that can lead to two types of queries:
   a. When the table consists of Party Identifier as an attribute, a simple record is required in the metadata query table.

      For example:

      Select v_party_id from Dim_Party where v_party_id='10'

   b. When the table does not consist of Party Identifier as an attribute, an interrelated set of records are required in the metadata query table AAI_DRF_QUERY_METADATA. Compose these set of records in a systematic way such that, for the selected Party Identifier, the table join procedure can be performed and traversed to reach the required PII attribute.



	ID	V_TABLE_NAME	V_COLUMN_NAME	V_CHILD_TABLE_NAME	V_CHILD_COLUMN_NAME	F_QUERY_FLAG	V_COLUMN_DATA_TYPE	V_TARGET_COLUMN_NAME	V_QUERY_NAME
1	1	Dim_Cards_Master	n_card_number_skey	Fct_Card_Acct_Mapping	n_card_number_skey	Y	number	v_d_cust_ref_code	Update_card_number
2	2	Fct_Card_Acct_Mapping	n_acct_skey	Fct_Cards_Summary	n_acct_skey	N	(null)	(null)	Update_card_number
3	3	Fct_Cards_Summary	n_cust_skey	Dim_Customer	n_cust_skey	N	(null)	(null)	Update_card_number
4	4	Dim_Email	n_email_skey	Fct_Party_Email_Map	n_email_skey	Y	varchar	v_party_id	Update_dim_email
5	5	Fct_Party_Email_Map	n_party_skey	Dim_Party	n_party_skey	N	(null)	(null)	Update_dim_email
6	6	Dim_Employee	(null)	(null)	(null)	(null)	varchar	v_employee_id	Update_dim_employee
7	7	Dim_Employee_Mls	(null)	(null)	(null)	(null)	varchar	v_employee_id	Update_dim_employee_ml
8	8	Dim_Phone	n_phone_skey	Fct_Party_Phone_Map	n_phone_skey	Y	varchar	v_party_id	Update_dim_phone
9	9	Fct_Party_Phone_Map	n_party_skey	Dim_Party	n_party_skey	N	(null)	(null)	Update_dim_phone

Table definition for AAI_DRF_QUERY_METADATA:

Column Name	Column Type	Description
ID	Number	This is the Primary Key field. You must enter a numerical value.
V_TABLE_NAME	Varchar	This is the source table name.
V_COLUMN_NAME	Varchar	This is the source column name.
V_CHILD_TABLE_NAME	Varchar	This is the table name, which must be linked to the V_TABLE_NAME. If the same table name is repeated with the same column name V_COLUMN_NAME, then the AND condition is formed with V_CHILD_TABLE_NAME. V_CHILD_TABLE_NAME

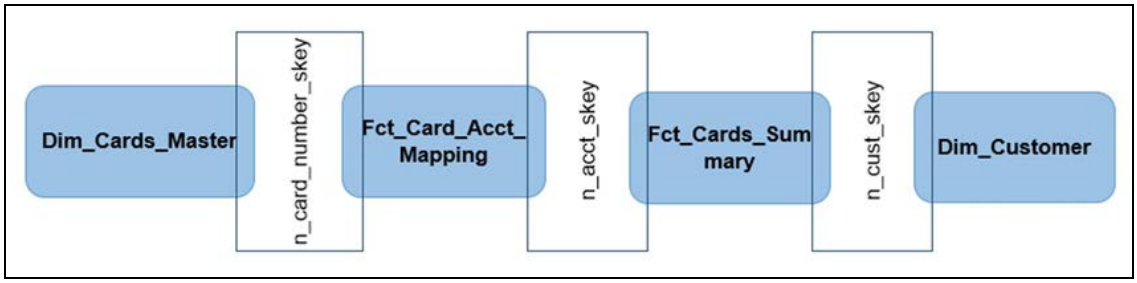
Column Name	Column Type	Description
V_CHILD_COLUMN_NAME	Varchar	This the column name, which must be linked to the V_COLUMN_NAME.
F_QUERY_FLAG	Varchar	Enter Y or N, which is case sensitive. If the value is Y, then you must form a query from V_TABLE_NAME .V_COLUMN_NAME
V_COLUMN_DATA_TYPE	Varchar	Mention the Data Type of the V_COLUMN_NAME. This is required only if F_QUERY_FLAG = Y.
V_TARGET_COLUMN_NAME	Varchar	Mention the PARTY_ID column name, which is required only if F_QUERY_FLAG = Y.
V_QUERY_NAME	Varchar	Mention the same query for a set of joining tables and columns. The set of tables and columns under join query are grouped together using the same query name.

For example:

Dim_Cards_Master table does not consist of n_cust_skey (n_cust_skey is the required Primary Key for the PII Attribute n_card_number_skey). Therefore, perform the table join procedure similar to the following query:

```
Select Dim_Cards_Master.n_card_number_skey from Dim_Cards_Master
Dim_Cards_Master, Fct_Card_Acct_Mapping Fct_Card_Acct_Mapping,

Fct_Cards_Summary Fct_Cards_Summary, Dim_Customer Dim_Customer where
Dim_Cards_Master.n_card_number_skey=Fct_Card_Acct_Mapping.n_card_number
_skey and
Fct_Card_Acct_Mapping.n_acct_skey=Fct_Cards_Summary.n_acct_skey and
Fct_Cards_Summary.n_cust_skey=Dim_Customer.n_cust_skey and
v_d_cust_ref_code='GDPR'
```



Where Dim_Customer.n_cust_skey is a Number Datatype.

NOTE For more sample queries generated using the query metadata table, see Sample Queries using the AAI_DRF_QUERY_METADATA Metadata Table.

To arrive at the above-mentioned query, follow these steps:

In first figure, the required table Dim_Cards_Master does not consist of Party Identifier. Therefore, perform the table join procedure using the AND condition at the table level.

i. Search for a table, which consists of the Party Identifier field. In this query, we have searched for the table Dim_Customer with unique identifier n_cust_skey field. This table must be joined with the required table Dim_Cards_Master.

ii. However, the tables Dim_Cards_Master and Dim_Customer do not consist of any common column name to perform the table join operation. Therefore, search for one more table Fct_Card_Acct_Mapping. This table (Fct_Card_Acct_Mapping) consists of common column name (n_card_number_skey) between Dim_Cards_Master table and itself.

iii. Join the Fct_Card_Acct_Mapping table, which consists of common column name (n_acct_skey) with another table Fct_Cards_Summary.

iv. Join the Fct_Cards_Summary table, which consists of common column name (n_cust_skey) with the final table Dim_Customer.

v. Now, the Dim_Cards_Master table is joined with the Dim_Customer table.

c. You must arrive at the skey or equivalent column in the table, which consists of the required PII attributes. Then the <<INFODOM>>_RightToForget batch uses this key to filter records (For example: Dim_Cards_Master) and randomize all the PIIs listed in the AAI_DRF_FUNCTION_COLUMN_MAP for that table.

4. Now, PII attributes can be queried and the values are randomized.

3.1.2 Sample Queries using the AAI_DRF_QUERY_METADATA Metadata table

These are the sample queries generated using the AAI_DRF_QUERY_METADATA table:

Example 1:

```
select DIM_MANAGEMENT.n_manager_skey from DIM_MANAGEMENT DIM_MANAGEMENT,
FCT_CUSTOMER FCT_CUSTOMER, DIM_CUSTOMER DIM_CUSTOMER where
DIM_MANAGEMENT.n_manager_skey=FCT_CUSTOMER.n_manager_skey and
FCT_CUSTOMER.n_cust_skey=DIM_CUSTOMER.n_cust_skey and
DIM_CUSTOMER.v_d_cust_ref_code in(?,?)
```

Example 2:

```
select  DIM_EMAIL.n_email_skey from DIM_EMAIL DIM_EMAIL, FCT_PARTY_EMAIL_MAP
FCT_PARTY_EMAIL_MAP, DIM_PARTY DIM_PARTY where
DIM_EMAIL.n_email_skey=FCT_PARTY_EMAIL_MAP.n_email_skey and
FCT_PARTY_EMAIL_MAP.n_party_skey=DIM_PARTY.n_party_skey and
DIM_PARTY.v_party_id in(?,?)
```

Example 3:

```
select  STG_CLAIM_DETAILS.v_claim_id from STG_CLAIM_DETAILS
STG_CLAIM_DETAILS, STG_CLAIM_CLAIMANT STG_CLAIM_CLAIMANT where
STG_CLAIM_DETAILS.v_claim_id=STG_CLAIM_CLAIMANT.v_claim_id and
STG_CLAIM_CLAIMANT.v_cust_ref_code in(?,?)
```

Example 4:

```
select STG_CONTACT_MASTER.v_contact_id from STG_CONTACT_MASTER
STG_CONTACT_MASTER, DIM_CONTACT DIM_CONTACT where
STG_CONTACT_MASTER.v_contact_id=DIM_CONTACT.v_contact_id and
DIM_CONTACT.v_customer_id in(?,?)
```

Example 5:

```
select  DIM_CARDS_MASTER.n_card_number_skey from DIM_CARDS_MASTER
DIM_CARDS_MASTER, FCT_CARD_ACCT_MAPPING FCT_CARD_ACCT_MAPPING,
FCT_CARDS_SUMMARY FCT_CARDS_SUMMARY where
DIM_CARDS_MASTER.n_card_number_skey=FCT_CARD_ACCT_MAPPING.n_card_number_skey
and FCT_CARD_ACCT_MAPPING. n_acct_skey=FCT_CARDS_SUMMARY.n_acct_skey and
FCT_CARDS_SUMMARY.v_d_cust_ref_code in(?,?)
```

3.1.3 Sample Query for the FSI_PARTY_RIGHT_TO_FORGET table

This is the sample entry for the FSI_PARTY_RIGHT_TO_FORGET table:

```
Insert into FSI_PARTY_RIGHT_TO_FORGET values (SYSDATE,
<<PARTY_ID_FROM_Ur_ENV>>, 'Testing Right2Forget');
```

3.2 Data Redaction

Data Redaction is one of the Data Security features that provides protection of data against unauthorized access and data theft.

In OFSAA, these tables are seeded as part of Data Redaction:

- AAI_DRF_FUNCTION_MASTER

  This table holds the Redaction function definitions. Generic logical functions can be address, email, card number, phone number etc.

- AAI_DRF_FUNCTION_COLUMN_MAP

  This table holds the Redaction Function- Column mappings. The PII columns will be redacted according to the Function mapping.

	V_FUNCTION_CD	V_TABLE_NAME	V_COLUMN_NAME	V_COLUMN_DATATYPE	V_COLUMN_DESC
53	ADDRESS	Dim_Party	v_ADDRESS_city	VARCHAR2(255)	Current / Residence ADDRESS...
54	ADDRESS	Dim_Party	v_ADDRESS_country	VARCHAR2(255)	Current / Residence ADDRESS...
55	ADDRESS	Dim_Party	v_ADDRESS_district	VARCHAR2(255)	Current / Residence ADDRESS...
56	ADDRESS	Dim_Party	v_ADDRESS_line_1	VARCHAR2(255)	Current / Residence ADDRESS...
57	ADDRESS	Dim_Party	v_ADDRESS_line_2	VARCHAR2(255)	Current / Residence ADDRESS...
58	ADDRESS	Dim_Party	v_ADDRESS_line_3	VARCHAR2(255)	Current / Residence ADDRESS...
59	ADDRESS	Dim_Party	v_ADDRESS_off_city	VARCHAR2(255)	Office ADDRESS City
60	ADDRESS	Dim_Party	v_ADDRESS_off_country	VARCHAR2(255)	Office ADDRESS Country
61	ADDRESS	Dim_Party	v_ADDRESS_off_district	VARCHAR2(255)	Office ADDRESS District
62	ADDRESS	Dim_Party	v_ADDRESS_off_line_1	VARCHAR2(255)	Office ADDRESS Line 1
63	ADDRESS	Dim_Party	v_ADDRESS_off_line_2	VARCHAR2(255)	Office ADDRESS Line 2
64	ADDRESS	Dim_Party	v_ADDRESS_off_line_3	VARCHAR2(255)	Office ADDRESS Line 3
65	ADDRESS	Dim_Party	v_ADDRESS_off_state	VARCHAR2(255)	Office ADDRESS State

- AAI_DRF_TABLE_ACCESS_CD_MAP

  This table holds the mapping of tables having columns marked for redaction to the Access codes. These access codes are SMS function codes and are expected to be mapped to the role DATASECURITY. The policy expression will be created based on this role and evaluated to access non-redacted data.

The list of PIIs, on which Data Redaction is applied, is available at My Oracle Support.

3.2.1 Accessing PII Table and PII Datasheet

- AAI_DRF_FUNCTION_COLUMN_MAP is the PII table.
- PII Datasheet list can be accessed from My Oracle Support.

3.2.2 Data Redaction Batch

Execute the Data Redaction seeded Batch ##INFODOM##_DATA_REDACTION to execute the Data Redaction Utility if it is available as part of application common metadata. If the Batch is not available, you must create a new Batch as mentioned in the Creating Batch for *Executing Data Redaction Utility* section in the OFS Analytical Applications Infrastructure Administration Guide.

The task in the Batch ##INFODOM##_DATA_REDACTION consists of three parameters:

- dataredaction.sh
- true/false
- OFSAA User ID

For more information, see Data Redaction section in the OFS Analytical Applications Infrastructure Administration Guide.

3.2.3 Mapping Roles to User Groups for Data Redaction

Data Controller Group is mapped to DATASECURITYADMIN role:

- Group Code: DATACONTROLLER
- Group Name: Data Controller Group
- Group Description: Data Controller Group
- Role code: DATASECURITYADMIN
- Role Name: Data Security Admin
- Role Description: Data security admin role for executing redaction policies

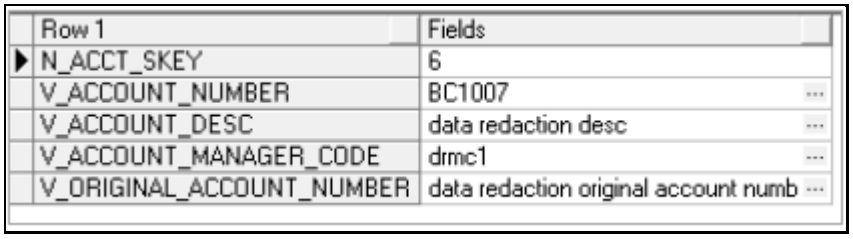
Mapping from individual applications to DATASECURITY role:

- Role code: DATASECURITY
- Role Name: Data Security Viewer
- Role Description: Data Security Viewer role for viewing original (non-redacted) data.

1. DATASECURITY role must be mapped to those application User Groups which have the privilege to view the data in its originality (un-redacted). Therefore, applications must identify the functions which must be mapped to the DATASECURITY role. These mappings must come as seeded data.
2. And then, map DATASECURITY role to the respective User groups. This mapping must be done manually from individual applications to the DATASECURITY role.

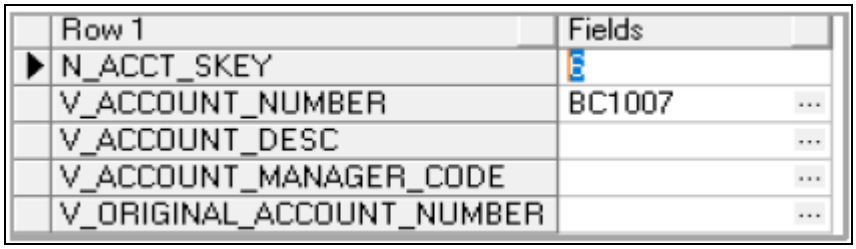
3.2.4 Data Redaction Batch Execution Sample

Data before executing Data Redaction Batch:



Row 1	Fields
N_ACCT_SKEY	6
V_ACCOUNT_NUMBER	BC1007
V_ACCOUNT_DESC	data redaction desc
V_ACCOUNT_MANAGER_CODE	drmc1
V_ORIGINAL_ACCOUNT_NUMBER	data redaction original account numb

Data after executing Data Redaction Batch:



Row 1	Fields
N_ACCT_SKEY	6
V_ACCOUNT_NUMBER	BC1007
V_ACCOUNT_DESC	
V_ACCOUNT_MANAGER_CODE	
V_ORIGINAL_ACCOUNT_NUMBER	

4 Reports Visibility for PCD Application OBIEE Reports

The Reports visibility for PCD application OBIEE Reports is restricted as per the table below:

Application Role	Dashboards	Tab	PII Availability
Business Analyst	Oracle Financial Services Price Creation and Discovery	Accounts Reviewed Deal Performance Offers Product Performance RM Performance	No No No No No
Administrator	All Dashboards	All Tabs and Reports	Yes

The Reports visibility for the different roles has to be handled by setting proper catalog Permissions. The steps to setup these permissions are described in Setting Up Dashboard Visibility under Configure Roles and Groups of this document.

NOTE Those users who have access to any of the above dashboards with PII columns should also be mapped to the 'Data Security Group' in OFSAA using SMS.

If PII entitlements change for a given user, then you need to either clear the cache through OBIEE admin or refresh the report.

5 Advanced User Access

Mapping Roles to User Groups for Data Redaction

Data Controller Group is mapped to **DATASECURITYADMIN** role:

- Group Code: DATACONTROLLER
- Group Name: Data Controller Group
- Group Description: Data Controller Group
- Role code: DATASECURITYADMIN
- Role Name: Data Security Admin
- Role Description: Data security admin role for executing redaction policies

Mapping from individual applications to **DATASECURITY** role:

- Role code: DATASECURITY
- Role Name: Data Security Viewer
- Role Description: Data Security Viewer role for viewing original (non-redacted) data.
    a. DATASECURITY role must be mapped to those application User Groups which have the privilege to view the data in its originality (un-redacted). Therefore, applications must identify the functions which must be mapped to the DATASECURITY role. These mappings must come as seeded data.
    b. And then, map DATASECURITY role to the respective User groups. This mapping must be done manually from individual applications to the DATASECURITY role.