

Oracle Flexcube Direct Banking

Data Protection Guide
Release 12.0.3.0.0

Part No. E52543_01

April 2014

ORACLE®

Data Protection Guide

April 2014

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2008, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Objective and Scope	4
1.1 Background	4
1.2 Objective	4
1.3 Scope	4
2. Personally Identifiable Information (PII)	5
3. Flow of PII Data	8
4. Administration of PII Data	10
4.1 Extracting PII data	10
4.1.1 Data stored in FCDB	10
4.2 Deleting or Purging PII data	11

1. Objective and Scope

1.1 Background

FCDB provides a unified, yet scalable channels banking solution for a bank to manage its data and end-to-end business operations.

In order to provide this service FCDB needs to acquire, use or store personally identifiable information (PII). In some cases, FCDB may be owner of the PII data and in some other cases FCDB might just acquire and use this data for providing required services to the customer.

1.2 Objective

By the very nature of PII data, it is necessary for the Bank to be aware of the information being acquired, used, or stored by FCDB. This knowledge will enable the Bank to take necessary measures and put apt policies and procedures in place to deal with PII data. In some of the geographies, the Bank might need to comply with local laws and regulations for dealing with PII data. This document attempts to provide necessary information to enable the Bank to do so.

1.3 Scope

This document is intended for technical staff of the Bank as well as administration users of the Bank and provides information about following aspects of the PII data.

- Identifies what PII data is acquired, used or stored in FCDB
- Flow of PII data

Out of scope

This document does not intend to suggest that FCDB is compliant with any local laws and regulations related to data protection. The purpose of this document is to provide information about PII data dealt with in the system so that the Bank can put in place appropriate processes to comply with laws and regulations of the land.

2. Personally Identifiable Information (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual.

FCDB needs to acquire, use or store some PII data of the customers of the Bank in order to perform its desired services. This section declares the PII data captured by FCDB so that the Bank is aware of the same and adopts necessary operational procedures and checks in order to protect PII data in the best interest of its customers.

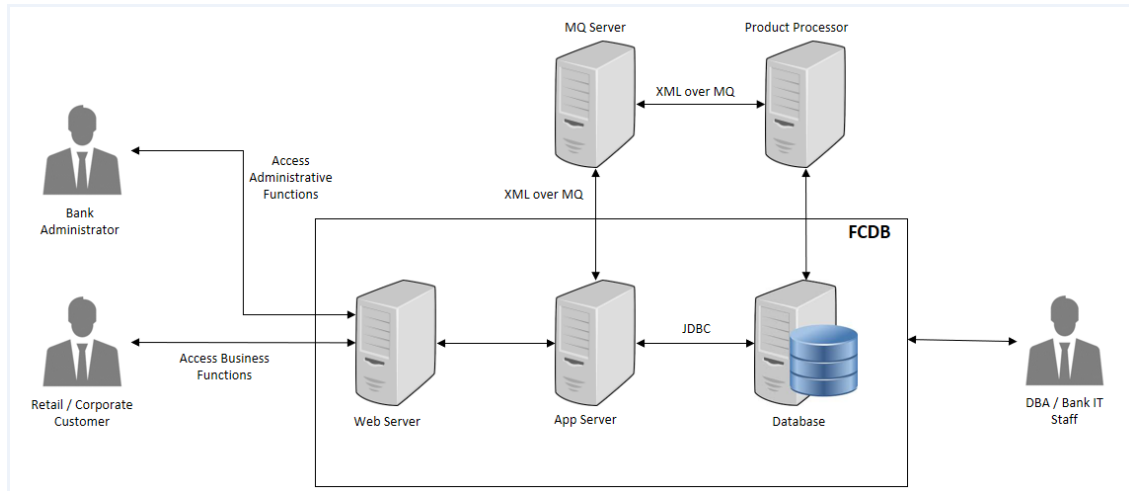
Fields	FCDB
Bank account information	Yes
Beneficiaries	Yes
Biometric records	No
Birthplace	No
Bonus	No
Country, state, or city of residence	Yes
Credit card numbers	Yes
Criminal record	No
Date of birth	Yes
Digital identity	No
Disability leave	No
Driver's license number	No
Education history	No
Email address	Yes
Emergency contacts	No
Employee ID	No
Ethnicity	No
Financial information and accounts	Yes

Fields	FCDB
Fingerprints	No
Full name	Yes
Gender	Yes
Genetic information	No
Health information (including conditions, treatment, and payment)	No
Healthcare providers and plans	No
Personal/office telephone numbers	Yes
IP address	No
Job title	Yes
Login name	Yes
MAC address	Yes
Marital status	Yes
Military rank	No
Mother's maiden name	Yes
National identification number	No
Passport number	No
Performance evaluation	No
Personal phone number	Yes
Photographic images	No
PIN numbers	Yes
Political affiliations	No

Fields	FCDB
Property title information	No
Religion	No
Salary	No
Screen name	No
Sexual life	No
Social security number	No
Taxpayer information	No
Union membership	No
Vehicle registration number	No
Work telephone	Yes
Citizenship Number	No
Geo-Location	No
Product has Customer defined fields	No
Mobile Subscriber Identifier (IMSI)	No
Surname	Yes
First name	Yes

3. Flow of PII Data

This section depicts the flow of 'personally identifiable information' (PII) within the FCDB system in the form of a data flow diagram.



The Bank Administrator is Bank's employee who is performing administrative functions using FCDB. As part of these, he will be dealing with PII data. An example is that the Administrator creates Retail and Corporate users in FCDB and while creating users, he enters user information such as first name, last name, email address, mobile number, correspondence address etc.

Retail / Corporate Customer is Bank's customer who is accessing the online banking features. As part of this he will be able to see his accounts, balances, beneficiaries, transactions, profile details etc.

DBA / Bank IT Staff is Bank's employee who is not a user of FCDB but has access to the database that stores FCDB back end data and/or the server environments on which FCDB is deployed.

Web server typically contains static web content such as styling information (CSS), Javascript resources, images, static HTMLs etc. However for the most part the Web Server acts as the Load Balancer.

Application (App) Server is the server on which FCDB services are deployed. This server performs required processing on the service calls. It uses the database for retrieval or storage of data. It can also connect to core product processor to inquire financial data or for posting any transactions initiated by the Retail/Corporate customer.

Database is the persistence store for FCDB. It can contain master configuration data, user data and transactional data.

Product Processor is the core banking solution, which actually processes banking transactions. FCDB connects to the product processor to fetch financial data or post online transactions.

4. Administration of PII Data

This section provides information about doing administrative tasks on PII data. This includes retrieval, modification, deletion or purging of such data.

4.1 Extracting PII data

4.1.1 Data stored in FCDB

This section provides information about the tables that store PII data. This information is useful for the Bank to extract PII information.

PII Data	Table
Bank account information	USERCUSTACCTTXNXREF USERCUSTREL ACCOUNTNICKNAMES ADMINTXNUNAUTHDATA BTFILEINFODET BTFILERECPMAP AUDITLOG HOSTAUDITLOG
Beneficiaries	MSTTEMPLATEMASTER
Country, state, or city of residence	MSTUSER
Date of birth	MSTUSER
Email address	MSTUSER
Full name	MSTUSER
Gender	MSTUSER
Personal/office telephone numbers	MSTUSER
Login name	MSTCHANNELUSER USERPIN
MAC Address	AUDITLOG
PIN numbers	USERPIN
Surname	MSTUSER

PII Data	Table
First name	MSTUSER

4.2 Deleting or Purging PII data

For some guidance on basic purging of data, please refer to https://docs.oracle.com/cd/E52543_01/PDF/Guide/Oracle_FLEXCUBE_Direct_Banking_Database%20Jobs.pdf

Purging of PII data can be done based on the knowledge of tables listed above and checking constraints and dependent tables.

However please note that it is not recommended to purge or delete any data stored in FCDB tables without doing detailed impact analysis. Please also note that the scheduled purge jobs are useful typically for purging old data. They may not be useful for purging data of a specific customer.