

Documentation Overview Guide

Oracle Financial Services:

Anti-Money Laundering | Fraud | Trading Compliance | Broker
Compliance | Energy and Commodity Trading Compliance | Know
Your Customer | FATCA Management | Currency Transaction
Reporting

Release 8.0.4.0.0

March 2017



Oracle Financial Services Behavior Detection Platform: **Documentation Overview Guide**

Release 8.0.4.0.0
March 2017

Document Number: E85851-01

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190

Document Number: E85851-01
First Edition (March 2017)

Copyright © 1996-2017, Oracle and/or its affiliates. All rights reserved.

Printed in U.S.A. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission.

Trademarks

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Oracle Financial Services Software, Inc.
1900 Oracle Way
13650 Dulles Technology Drive
Phone: (703) 478-9000
Fax: (703) 318-6340
Internet: www.oracle.com/financialservices

Contents

List of Tables	v
About this Guide	1
Who Should Use this Guide	1
Scope of this Guide.....	3
How this Guide is Organized.....	3
CHAPTER 1 Administration Guide	7
Who Should Use this Guide	7
Scope of this Guide.....	8
How this Guide is Organized.....	8
Where to Find More Information	9
CHAPTER 2 Administration Tools User Guide	11
Who Should Use this Guide	11
Scope of this Guide.....	11
How this Guide is Organized.....	11
Where to Find More Information	12
CHAPTER 3 Configuration Guide	13
Who Should Use this Guide	13
How this Guide is Organized.....	14
Where to Find More Information	15
CHAPTER 4 Scenario Wizard Configuration Guide	17
Who Should Use this Guide	17

How this Guide is Organized	17
Where to Find More Information	18
CHAPTER 5 Data Interface Specification	19
About this Guide	19
Who Should Use this Guide	19
How this Guide is Organized	20
Where to Find More Information	21
CHAPTER 6 FSDM Reference Guide, Volume 1: Business Data	23
Who Should Use this Guide	23
Scope of this Guide.....	23
How this Guide is Organized	24
Where to Find More Information	24
CHAPTER 7 FSDM Reference Guide, Volume 2: Oracle Financial Services Data27	
Who Should Use this Guide	27
Scope of this Guide.....	28
Where to Find More Information	28
CHAPTER 8 FSDM Reference Guide, Volume 3: Case Management Data	29
Who Should Use this Guide	29
Scope of this Guide.....	29
Where to Find More Information	30
CHAPTER 9 Installation Guide	31
About this Guide	31
Who Should Use this Guide	31
Prerequisites.....	32
How this Guide is Organized	32
Where To Find More Information	34
CHAPTER 10 Release Notes	35
About this Guide	35
Who Should Use this Guide	36
How this Guide is Organized	36
Where to Find More Information	36
CHAPTER 11 Scenario Manager User Guide	39

Who Should Use this Guide	39
Scope of this Guide.....	39
How this Guide is Organized.....	40
Where to Find More Information	41
CHAPTER 12 <i>Security Guide</i>	43
Who Should Use this Guide	43
Scope of this Guide.....	43
How this Guide is Organized.....	43
Where to Find More Information	44
CHAPTER 13 <i>Alert Management User Guide</i>	47
Who Should Use this Guide	47
How this Guide is Organized.....	48
Where to Find More Information	49
CHAPTER 14 <i>Enterprise Case Management User Guide</i>	51
Who Should Use this Guide	51
How this Guide is Organized.....	52
Where to Find More Information	53
CHAPTER 15 <i>Personal Trading Approval User Guide</i>.....	55
Who Should Use this Guide	55
How this Guide is Organized.....	55
Where to Find More Information	56
CHAPTER 16 <i>Glossary of Financial Crime and Compliance Management Products</i>57	
About this Guide.....	57
Who Should Use this Guide	57
CHAPTER 17 <i>Services Guide</i>.....	59
Who Should Use this Guide	59
How this Guide is Organized.....	59
Where to Find More Information	60
CHAPTER 18 <i>Technical Scenario Description - Anti-Money Laundering Solution</i>61	
About this Guide.....	61
Who Should Use this Guide	62

How this Guide is Organized	63
CHAPTER 19 Technical Scenario Description - Broker Compliance	65
About this Guide	65
Who Should Use this Guide	66
How this Guide is Organized	67
CHAPTER 20 Technical Scenario Description - Currency Transaction Reporting 69	
About this Guide	69
Who Should Use this Guide	70
How this Guide is Organized	71
CHAPTER 21 Technical Scenario Description - Energy and Commodity Trading Compliance 73	
About this Guide	73
Who Should Use this Guide	74
How this Guide is Organized	75
CHAPTER 22 Technical Scenario Description - Fraud Detection	77
About this Guide	77
Who Should Use this Guide	78
How this Guide is Organized	79
CHAPTER 23 Technical Scenario Description - Trading Compliance	81
About this Guide	81
Who Should Use this Guide	82
How this Guide is Organized	83
APPENDIX A Know Your Customer	85
About KYC	85
APPENDIX B Currency Transaction Reporting	87
About CTR	87
APPENDIX C FATCA Management	89
About FATCA Management.....	89

List of Tables

Table 1. Who Should Use This Guide.....	1
Table 2. Oracle Financial Services Behavior Detection Documentation Overview.....	3

About this Guide

This guide explains the Oracle Financial Services suite of documentation products, including User Guides, Online Help, and ReadMe files.

This chapter covers the following topics:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized

Who Should Use this Guide

The *Oracle Financial Services Documentation Overview Guide* is designed for people interested in the Oracle Financial Services documentation set. The Oracle Financial Services application is released with over 40 different documents.

This overview provides a high-level description of each document.

Table 1. Who Should Use This Guide

	Oracle Installer	System Admin.	Data Miner	Oracle Admin	IT Support Staff	Oracle Pro. Services Team	Business Analyst	Oracle Dev Team	Active Pages Dev.	System Integrator	Analyst	Auditor	Executive	Supervisor
Administration Guide	x	x												
Administrator Tools Guide			x	x										
Alert Management User Guide										x	x	x	x	
Configuration Guide	x			x										
CTR Administration and Configuration Guide	x	x												
CTR User Guide										x	x	x	x	
Data Interface Specification			x		x	x								
ECM User Guide										x	x	x	x	
FATCA Management Administration and Configuration Guide	x	x												

**Who Should Use this Guide
About This Guide**

Table 1. Who Should Use This Guide

	Oracle Installer	System Admin.	Data Miner	Oracle Admin	IT Support Staff	Oracle Pro. Services Team	Business Analyst	Oracle Dev Team	Active Pages Dev.	System Integrator	Analyst	Auditor	Executive	Supervisor
FATCA Management Data Model Reference Guide					x	x	x	x						
FATCA Risk Assessment Guide											x	x	x	x
FSDM Reference Guide, Vol. 1					x	x	x	x						
FSDM Reference Guide, Vol. 2					x	x	x	x						
FSDM Reference Guide, Vol. 3					x	x	x	x						
BD App Pack Installation Guide	x	x												
KYC Administration and Configuration Guide	x	x												
KYC Data Model Reference Guide					x	x	x	x						
KYC Risk Assessment Guide											x	x	x	x
KYC Services Guide									x	x				
PTA User Guide											x	x	x	x
Release Notes	x	x												
Scenario Manager User Guide			x											
Scenario Wizard Configuration Guide			x											
SecurityGuide		x												
Services Guide									x	x				
Technical Scenario Descriptions (all)			x	x	x	x	x	x			x	x	x	x

Scope of this Guide

The *Documentation Overview Guide*, is designed for users of the Oracle Financial Services Behavior Detection Applications Pack.

Table 2. Oracle Financial Services Behavior Detection Documentation Overview

Back-End Documents	Front-End Documents
Administration Guide	Alert Management User Guide
Administration Tools User Guide	Currency Transaction Reporting User Guide
Configuration Guide	Enterprise Case Management User Guide
Currency Transaction Reporting Administration and Configuration Guide	FATCA Assessment Guide
Data Interface Specification	Glossary
FATC Management Administration and Configuration Guide	KYC Risk Assessment Guide
FATCA Management Data Model Reference Guide	KYC Services Guide
FSDM Reference Guide Vol 1: Business Data	Personal Trading Approval User Guide
FSDM Reference Guide Vol 2: Oracle Financial Services Data	Services Guide
FSDM Reference Guide Vol 3: Case Management Data	TSD - Anti Money Laundering
Installation Guide	TSD - Broker Compliance
KYC Administration Guide	TSD - Currency Transaction Reporting
KYC Data Model Reference Guide	TSD - Energy and Commodity Trading Compliance
Release Notes	TSD - Fraud Detection
Scenario Manager User Guide	TSD - Trading Compliance
Scenario Wizard Configuration Guide	
Security Guide	

How this Guide is Organized

The *Documentation Overview Guide* includes the following chapters:

Back-End Documents

- Chapter 1, *Administration Guide*, on page 7
- Chapter 2, *Administration Tools User Guide*, on page 11
- Chapter 3, *Configuration Guide*, on page 13
- Chapter 4, *Scenario Wizard Configuration Guide*, on page 17
- Chapter 5, *Data Interface Specification*, on page 19
- Chapter 6, *FSDM Reference Guide, Volume 1: Business Data*, on page 23
- Chapter 7, *FSDM Reference Guide, Volume 2: Oracle Financial Services Data*, on page 27
- Chapter 8, *FSDM Reference Guide, Volume 3: Case Management Data*, on page 29

- Chapter 8, *Installation Guide*, on page 31
- Chapter 9, *Release Notes*, on page 35
- Chapter 10, *Scenario Manager User Guide*, on page 39
- Chapter 11, *Security Guide*, on page 43

Front-End Documents

- Chapter 11, *Alert Management User Guide*, on page 47
- Chapter 12, *Enterprise Case Management User Guide*, on page 51
- Chapter 13, *Personal Trading Approval User Guide*, on page 55
- Chapter 14, *Glossary of Financial Crime and Compliance Management Products*, on page 57
- Chapter 12, *Services Guide*, on page 59
- Chapter 13, *Technical Scenario Description - Anti-Money Laundering Solution*, on page 61
- Chapter 14, *Technical Scenario Description - Broker Compliance*, on page 65
- Chapter 15, *Technical Scenario Description - Currency Transaction Reporting*, on page 69
- Chapter 16, *Technical Scenario Description - Energy and Commodity Trading Compliance*, on page 73
- Chapter 17, *Technical Scenario Description - Fraud Detection*, on page 77
- Chapter 18, *Technical Scenario Description - Trading Compliance*, on page 81

Application-specific Documents

- Appendix A, *Know Your Customer*, on page 85
- Appendix B, *Currency Transaction Reporting*, on page 87
- Appendix C, *FATCA Management*, on page 89

Part 1: Back-End Documents

This guide explains the concepts behind Oracle Financial Services Behavior Detection (OFSBD), and provides comprehensive instructions for proper system administration, as well as daily operations and maintenance. This section focuses on the following topics:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information

For installation and configuration information about Sun Java System, BEA, and Apache software, refer to the appropriate documentation that is available on the associated web sites.

Who Should Use this Guide

This *Administration Guide* is designed for use by the Installers and System Administrators. Their roles and responsibilities, as they operate within OFSBD, include the following:

- **Installer:** Installs and configures OFSBD at a specific deployment site. The Installer also installs and upgrades any additional Oracle Financial Services solution sets, and requires access to deployment-specific configuration information (For example, machine names and port numbers).
- **System Administrator:** Configures, maintains, and adjusts the system, and is usually an employee of a specific Oracle customer. The System Administrator maintains user accounts and roles, monitors data ingestion and alert management, archives data, loads data feeds, and performs post-processing tasks. In addition, the System Administrator can reload cache. However, the scenario description is not visible to the System Administrator.

Note: Administrators who have access to any of the Financial Crime and Compliance Management (FCCM) modules, such as Enterprise Case Management, Anti-Money Laundering, Fraud, and so on, will get unrestricted access to the administration utilities that are required to administer the module.

Scope of this Guide

This guide describes the physical and logical architecture of the OFSBDF. It also provides instructions for installing and configuring OFSBD, its subsystem components, and any third-party software required for operation.

OFSBD is powered by advanced data mining algorithms and sophisticated pattern recognition technologies. It provides an open and scalable infrastructure that supports rich, end-to-end functionality across all Oracle Financial Services solution sets. OFSBD's extensible, modular architecture enables a customer to deploy new solution sets readily as the need arises.

This guide provides information about how to administer the following products:

- Anti-Money Laundering (AML)
- Fraud
- Energy and Commodity Trade Compliance (ECTC)
- Broker Compliance (BC)
- Trader Compliance (TC)
- Enterprise Case Management (ECM)
- Personal Trading Approval

Your implementation may not be utilizing all of these products.

How this Guide is Organized

The *Administration Guide*, includes the following chapters:

- *Chapter 1, About Oracle Financial Services Behavior Detection (OFSBD)*, provides a brief overview of the Oracle Financial Services Framework and its components.
- *Chapter 2, Managing User Administration and Security Configuration*, covers the required day-to-day operations and maintenance of OFSBD users, groups, and organizational units.
- *Chapter 3, Managing Data*, describes the operation and process flow of data management subsystem components.
- *Chapter 4, Behavior Detection Jobs*, provides an overview of the OFSBD Job Protocol and procedures for performing various tasks that relate to starting, stopping, and recovering jobs.
- *Chapter 5, Post-Processing Tasks*, explains how to customize the OFSBD features that affect presentation of user information on the desktop.
- *Chapter 6, Managing Batch Processing Utilities*, provides information about the OFSBD utilities related to the batch process.
- *Chapter 7, Managing Administrative Utilities*, provides information about the OFSBD utilities that are independent of the batch process.
- *Chapter 8, Posting External Alerts through Batches*, provides information about how to post alerts from an external system into the OFSBD.

- Chapter 9, *Alert Generation from IPE Assessment Results*, provides information about how to generate alerts using the Inline Processing Engine (IPE) Assessments.
- Appendix A, *Logging*, describes the OFSBD logging features.
- Appendix B, *OFSBD Software Updates*, describes the application of OFSBD software updates (hotfix) and their impact on customization.
- Appendix C, *User Administration*, describes the user administration of the Oracle Financial Services Behavior Detection.
- Appendix D, *Managing Data*, describes the BDF file parameters, the FSDF datamaps, the Data Quality group names and related T2T names, the BDF interface files, and the directory structures.
- Appendix E, *Managing Additional Data Processing Activities*, describes the additional data processing activities that can be performed in the BD applications.
- Appendix F, *BDF Datamap Details*, lists the Datamap XML and their use in OFSBD.
- Appendix G, *Datamaps Matrix*, lists which datamaps are required for each solution set.
- Appendix H, *Configuring Administration Tools*, describes how to configure the Administration Tools feature.
- Appendix I, *Mapping Compliance Regulatory Reports Actions*, provides information about integration of OFSRRS.
- Appendix J, *Alerts from IPE and External System - Run/Process/Tasks*, provides information about integration of the Inline Processing Engine.
- The *Index* provides an alphabetized cross-reference list that helps you locate information quickly.

Where to Find More Information

For more information about Oracle Financial Services, refer to the following Behavior Detection application documents, which can be found at

http://docs.oracle.com/cd/E60570_01/homepage.htm:

- *Scenario Manager User Guide*
- *Administration Tools User Guide*
- *Services Guide*
- *Data Interface Specification (DIS)*
- *Configuration Guide*
- *Installation Guide*

Additionally, you may find pertinent information in the OFSAAI documentation, found at the following link:

http://docs.oracle.com/cd/E60058_01/homepage.htm:

- *Oracle Financial Services Analytical Applications Infrastructure User Guide*
- *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration*

For installation and configuration information about Sun Java System, BEA, and Apache software, refer to the appropriate documentation that is available on the associated web sites.

This guide identifies the Administration Tools used with the Oracle Financial Services Behavior Detection Platform, and describes how to use them. This chapter details the following:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Administration Tools User Guide*, is designed for data miners and Oracle Administrators. Their roles and responsibilities include the following:

- **Data Miner:** Accesses the Administration Tools to modify the threshold values used by patterns to detect matches in Firm data.
- **Oracle Administrator:** Accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. In addition, Oracle Administrators can reload the cache. This user is usually an employee of a specific Oracle customer.

Scope of this Guide

This guide describes how to use the Administration Tools to customize the scenario threshold, alert creation, alert scoring, and alert and case assignment criteria.

How this Guide is Organized

The *Administrator Tools User Guide*, includes the following chapters:

- Chapter 1, *Overview of FCCM*, provides an overview of Oracle Financial Services Financial Crimes and Compliance Management, how it works, and what it does.
- Chapter 2, *About the Administration Tools*, describes how to access the tools and identifies what elements are common to all tools.
- Chapter 3, *Scenario Threshold Editor*, describes how to use this tool to modify the threshold values
- Chapter 4, *Scenario Wizard*, describes how to use the Scenario Wizard tool to create scenarios.
- Chapter 5, *Alert Creator Editor*, describes how to use this tool to automatically group the matches that share similar information into a single alert. It also explains how to create new rules, modify the logic behind existing rules, and delete rules. The tool also displays the job ID and the job template ID for all the rules created.
- Chapter 6, *Alert Scoring Editor*, describes how to create new rules or modify the logic behind existing rules that prioritize alerts automatically.

- Chapter 7, *Alert Assigner Editor*, describes how to assign ownership of alerts.
- Chapter 8, *Case Assigner Editor*, describes how to assign ownership of cases.
- Chapter 9, *Threshold Analyzer*, introduces you the Threshold Analyzer utility and describes how to view and operate the source business and Threshold Analyzer data.
- Chapter 10, *Security Configuration*, covers the required day-to-day operations and maintenance of OFSBDF users, groups, and organizational units.
- Chapter 11, *Inline Processing Engine (IPE) Scenario Configuration*, describes how to create scenarios using Inline Processing Engine (IPE).
- The *Index* provides access to specific topics for this tool.

Where to Find More Information

For more information about Oracle Financial Services Behavior Detection Framework, refer to the following documents:

- *Installation Guide*
- *Oracle Financial Services Advanced Analytical Applications Infrastructure (OFS AAI) Applications Pack Installation and Configuration Guide*
- *Scenario Manager User Guide*
- *Services Guide*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about the Oracle Financial Services and complete product line, visit Web site at www.oracle.com/financialservices.

This guide explains the structure behind the Oracle Financial Services Behavior Detection Platform and Oracle Financial Services Enterprise Case Management user interface (UI) and provides comprehensive instructions for configuring modifiable components. This chapter focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Configuration Guide* is designed for use by application users and client personnel who have a working knowledge of eXtensible Markup Language (XML) and UI software components. Their roles and responsibilities, as they operate within the Oracle Financial Services Behavior Detection Framework and Oracle Financial Services Enterprise Case Management, include the following:

- **Installers:** Installs and configures the Oracle Financial Services Behavior Detection Platform and Oracle Financial Services Enterprise Case Management at a specific deployment site. The Oracle Financial Services application Installer also requires access to deployment-specific configuration information (for example, machine names and port numbers).
- **Administrators:** Configures, maintains, and adjusts the Oracle Financial Services Behavior Detection Platform and Oracle Financial Services Enterprise Case Management user interface, and is usually an employee of a specific Oracle Financial Services customer.

How this Guide is Organized

The *Configuration Guide* includes the following chapters:

- Chapter 1, *General Configuration* provides instructions for configuring general items that are reflected throughout the UI, such as, default settings that are configurable within the UI.
- Chapter 2, *Alert Management Configuration* provides instructions for configuring the parameters specific to alert management.
- Chapter 3, *Administration Tools Configuration* provides instructions for configuring the parameters specific to administration tools.
- Chapter 4, *Case Management Configuration* provides instructions for configuring the parameters specific to case management.
- Chapter 5, *Assessment Configuration* provides instructions for configuring the parameters specific to risk assessment.
- Chapter 6, *KYC Risk Assessment Configuration* provides instructions on configuring the weights of the risk assessment parameters per customer type for different risk models available in KYC.
- Chapter 7, *Actions Configuration* provides instructions for configuring the Action page of the UI.
- Chapter 8, *Web Application Configuration* provides instructions for configuring the functional settings of the Web Application for the UI post installation.
- Chapter 9, *OBIEE Report Configuration* provides instructions for configuring Oracle Financial Services Analytic reports and graphs.
- The *Index*, provides an alphabetized cross-reference list that helps you locate information quickly.

Where to Find More Information

For more information about Oracle Financial Services Behavior Detection Platform, refer to the following documents:

- Administration Guide
- Administration Tools User Guide
- Scenario Manager User Guide
- Installation Guide
- Alert Management User Guide
- Enterprise Case Management User Guide
- KYC Risk Assessment Guide

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

This guide explains the structure behind the Oracle Financial Services Scenario Wizard and provides comprehensive instructions for configuring modifiable components.

This chapter focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Scenario Wizard Configuration Guide* is designed for use by application users and client personnel who have a working knowledge of eXtensible Markup Language (XML) and UI software components. Their roles and responsibilities, as they operate within the Oracle Financial Services Enterprise Case Management, include the following:

- **Data Miner:** Configures, maintains, and adjusts the Oracle Financial Services Behavior Detection Framework and Oracle Financial Services Alert Management user interface, and is usually an employee of a specific Oracle Financial Services customer.

How this Guide is Organized

The *Scenario Wizard Configuration Guide* includes the following chapters:

- Chapter 1, *About Scenario Wizard*, provides a brief introduction about the Oracle Financial Services Scenario Wizard tool.
- Chapter 2, *Template XML Files*, explains the Template XML files, their structure, content, and inter-relationship. It also describes the configurations that need to be done for scaling out-of-the-box options.
- Chapter 3, *Scenario Focus Mapping (ScenarioFocusMapping.xml)*, explains about the different configurations using ScenarioFocusMapping.xml file.
- Chapter 4, *Threshold (threshold.xml)*, describes the tags used by the threshold.xml file.
- Chapter 5, *TA Column Map (TAColumnMap.xml)*, describes the tags used by the TAColumnMap.xml file.
- Chapter 6, *Data Set Rule Map (datasetrulemap.xml)*, explains about the different configurations using datasetrulemap.xml file.
- Appendix A, *Embedding Queries in XML*, shows how to edit XML with simple SQL query.

- Appendix B, *Using Functions in Query*, shows the usage of aggregate functions inside SQL query.
- Appendix C, *Nested Query*, shows the usage of nested query inside the SQL.

Where to Find More Information

For more information about Oracle Financial Services Behavior Detection Framework, refer to the following documents:

- *Administration Guide*
- *Administration Tools User Guide*
- *Scenario Manager User Guide*
- *Installation Guide*
- *Alert Management User Guide*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

The *Oracle Financial Services Data Interface Specification (DIS)* identifies the super-set of data (that is, data files and file content) that the Oracle client supplies for data ingestion. This guide describes the major components of the system, defines acronyms used through the specification, and lists supplemental reference material.

This chapter focuses on the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

About this Guide

The *Data Interface Specification (DIS)* specifies the data interface between the Oracle Financial Services Behavior Detection Platform Data Ingestion subsystem and the client's internal or external systems that provide data to the Financial Services Data Model (FSDM).

The DIS defines how, and in what format, the client must provide source business data and market data to the Ingestion Manager. The DIS specifies the protocols that the Ingestion Manager uses to recognize data arrival, to understand its context, and to validate the data content. The DIS describes the interface at a level of detail that enables the client to design and implement processes and procedures for delivery of source business data to Oracle Financial Services.

This guide describes the format and content of the data the Ingestion Manager uses. This data is provided in the form of text files of market data. The Ingestion Manager receives and processes this source data making it available to the other Oracle Financial Services components, which provide behavior detection and alert management related to your trading and payments activity.

Who Should Use this Guide

The *Data Interface Specification* is designed for use by Oracle Financial Services and client personnel who are involved with the ingestion process. Their roles and responsibilities include the following:

- **IT Support Staff:** Identify the appropriate client data sources that Oracle Financial Services requires, develop any processes needed to extract that data in the form that Oracle Financial Services requires, and deliver that data to Oracle Financial Services.
- **Oracle Financial Services Professional Services Team:** Is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.

- **System Administrator:** Configures, maintains, and adjusts the system and is usually an employee of a specific Oracle Financial Services client. The System Administrator maintains user accounts and roles, archives data, and loads data feeds.

How this Guide is Organized

The *Data Interface Specification* is organized as follows:

- Chapter 1, *Data Exchange Specification*, identifies the data files required by the Ingestion Manager and the exchange protocols used to provide these data files. Specific details such as naming conventions and data delivery timing are specified.
- Chapter 2, *Architecture Overview*, describes the logical architecture of the interface between your systems and the Ingestion Manager.
- Chapter 3, *Data Format and Conventions Specification*, describes the content and format of the data files that are submitted to the Ingestion Manager. Additionally, it provides general and specific data format guidelines that are applied to the data files.
- Chapter 4, *Account Data*, provides detailed format specifications for each of the Account data files, the set of valid field values for those fields in which Oracle specifies the values, and any supplementary guidance required for creating the data files.
- Chapter 5, *Customer Data*, provides detailed format specifications for each of the Customer data files, the set of valid field values for those fields in which Oracle specifies the values, and any supplementary guidance required for creating the data files.
- Chapter 6, *Enterprise Data*, provides detailed format specifications for each of the Enterprise data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.
- Chapter 7, *Security Data*, provides detailed format specifications for each of the Security data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.
- Chapter 8, *Market Data*, provides detailed format specifications for each of the Market data files, the set of valid field values for those fields in which Oracle specifies the values, and any supplementary guidance required for creating the data files.
- Chapter 9, *Trade Data*, provides detailed format specifications for each of the Trade data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.
- Chapter 10, *Energy and Commodity Trading Compliance Data*, provides detailed format specifications for each of the Energy and Commodity Trading Compliance data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.
- Chapter 11, *Transaction Data*, provides detailed format specifications for each of the Transaction data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.
- Chapter 12, *Currency Transaction Reporting Data*, provides detailed format specifications for each of the Currency Transaction Reporting data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.

- Chapter 13, *Trade Finance Data*, provides detailed format specifications for each of the Trade Finance data files, the set of valid field values for those fields in which Oracle specifies the values, and any required supplementary guidance for creating the data files.
- Chapter 14, *Data Mart Initialization*, describes the content and format of data required for the initial loading of the Data Mart. Historical source and summary data are required to support initial production operations of Oracle Financial Services products. This chapter specifies what and how that historical data is to be provided to the Ingestion Manager.
- The *Index* provides an alphabetized cross-reference list that helps you locate information quickly.

Where to Find More Information

For more information about Oracle Financial Services Behavior Detection Platform, refer to the following documents:

- *Scenario Manager User Guide*
- *Installation Guide*
- *Administration Tools User Guide*
- *Alert Management User Guide*
- *Enterprise Case Management User Guide*
- *Currency Transaction Reporting User Guide*
- *FSDM Reference Guide, Vol.1, Business Data*
- *FSDM Reference Guide, Vol.2, Oracle Financial Services Data*
- *FSDM Reference Guide, Vol.3, Case Management Data*
- *Services Guide*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

FSDM Reference Guide, Volume 1: Business Data

This chapter provides a brief overview of the purpose, scope, and organization of this document.

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Financial Services Data Model Reference Guide, Volume 1, Business Data* is designed for use by Oracle client Business Analysts and Information Technology (IT) Support Staff, as well as for use by the Oracle Professional Services and Development Teams. Their roles and responsibilities include the following:

- **Business Analyst:** A user in this role analyzes and dispositions the alerts that Oracle Financial Services Behavior Detection generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle.
- **IT Support Staff:** A user in this role is responsible for identifying the appropriate client data sources that Oracle requires, developing any processes needed to extract that data in the form Oracle requires, and delivering that data.
- **Oracle Professional Services Team:** A user in this role is responsible for the deployment of Oracle at the client's installation site. The Oracle Professional Services Team provides guidance and assistance in the identification and delivery of data.
- **Oracle Development Team:** A user in this role is responsible for developing Oracle scenarios and user interface, which are based entirely on the data that the FSDM provides.

Scope of this Guide

This guide describes how the data in the FSDM is organized, how Oracle uses the data, and how to achieve specific business outcomes with the data.

How this Guide is Organized

The *Financial Services Data Model Reference Guide, Volume 1, Business Data*, is organized as follows:

- Chapter 1, *Introduction*, details elements that many of the subject areas share within the FSDM.
- Chapter 2, *Account Data*, details how account-related data is stored in the FSDM.
- Chapter 3, *Customer Data*, details how customer-related data is stored in the FSDM.
- Chapter 4, *Enterprise Data*, details how enterprise-related data is stored in the FSDM.
- Chapter 5, *Security Data*, details how security-related data is stored in the FSDM.
- Chapter 6, *Market Data*, details how market-related data is stored in the FSDM.
- Chapter 7, *Transaction Data*, details how transaction-related data is stored in the FSDM.
- Chapter 8, *Trade Data*, details how trade-related data is stored in the FSDM.
- Chapter 9, *Energy and Commodity Trading Data*, details how trade-related data is stored in the FSDM.
- Chapter 10, *Currency Transaction Reporting Data*, details how currency transaction reporting data is stored in the FSDM.
- Chapter 11, *Trade Finance Data*, details how trade finance data is stored in the FSDM.

Where to Find More Information

For more information about Oracle Behavior Detection and the FSDM, refer to the following documents:

- The *Data Interface Specification (DIS)* identifies the set of business data files that are required for each Oracle solution set and specifies the proper format in which the data is to be provided such that the system can ingest it.
- The *Administration Guide* explains how the software works, and provides instructions for configuring Oracle, its subcomponents, and required third-party software for operation. With respect to the FSDM specifically, it describes the steps by which data is processed and loaded (ingested) into the database.
- The *Oracle Anti-Money Laundering Scenario to DIS Data Map*, *Oracle Trading Compliance Scenario to DIS Data Map*, *Oracle Broker Compliance Scenario to DIS Data Map*, and *Oracle Fraud Scenario to DIS Data Map* identify the set of business data attributes that are required for each scenario in a particular solution set.
- The *Oracle Anti-Money Laundering Technical Scenario Descriptions*, *Oracle Trading Compliance Technical Scenario Descriptions*, *Oracle Broker Compliance Technical Scenario Descriptions*, *Oracle Fraud Technical Scenario Descriptions*, *Oracle Currency Transaction Reporting Technical Scenario Descriptions*, *Oracle Energy and Commodity Trading Compliance Technical Scenario Descriptions*, and *Oracle Currency Transaction Reporting Technical Scenario Descriptions* provide a detailed technical definition of each scenario in a specific Oracle solution set, including the relation of the data to the behavior of interest that the scenario is monitoring.
- The *Financial Services Data Model Reference Guide, Volume 2, Oracle Financial Services Data* defines the tables Oracle uses to capture and store Oracle operations data, including scenario meta data and resulting alerts. The *Financial Services Data Model Reference Guide, Volume 3, Case Management Data* defines the tables Oracle uses to capture and store Case Management data, including scenario meta data and resulting alerts.

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

FSDM Reference Guide, Volume 2: Oracle Financial Services Data

This chapter provides a brief overview of the purpose, scope, and organization of this document.

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide

Who Should Use this Guide

The *Financial Services Data Model Reference Guide, Volume 2, Oracle Financial Services Data* is designed for use by Oracle Business Analysts and Information Technology (IT) Support Staff, as well as for use by the Oracle Professional Services and Development Teams. Their roles and responsibilities include the following:

- **Business Analyst:** This user analyzes and dispositions the alerts that the Oracle Financial Services Behavior Detection Platform™ (herein referred to as Behavior Detection) generates. The Business Analyst needs a semantic understanding of the data provided in the Financial Services Data Model (FSDM) to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Behavior Detection.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Behavior Detection requires, developing any processes needed to extract that data in the form the system requires, and delivering that data.
- **Professional Services Team and Partners:** This user is responsible for the deployment of Behavior Detection at the client's installation site. The Professional Services Team provides guidance and assistance in the identification and delivery of data

Scope of this Guide

This guide describes how the data in the FSDM is organized, how Oracle Financial Services uses the data, and how to achieve specific business outcomes with the data.

How this Guide is Organized

The *Financial Services Data Model Reference Guide*, Volume 2, *Oracle Financial Services Data* is organized as follows:

- *Chapter 1, Introduction*, details elements that many of the subject areas share within the FSDM.
- *Chapter 2, Behavior Detection*, details how scenario-related data is stored in the FSDM.
- *Chapter 3, Detection Results*, details how detection results-related data is stored in the FSDM.
- *Chapter 4, Investigation Management*, details how investigation management-related data is stored in the FSDM.
- *Chapter 5, Investigation Management Configuration*, details how investigation management configuration-related data is stored in the FSDM.
- *Chapter 6, Common Processing*, describes common tables used to create the data for Behavior Detection, Detection Results, and Investigation Management.
- *Chapter 7, Trade Blotter*, details how trade blotter-related data is stored in the FSDM.
- *Chapter 8, Regulatory Reporting*, details how the optional Regulatory Reporting application-related data is stored in the FSDM.
- *Chapter 9, Control Room*, details how the Control Room-related data is stored in the FSDM.

Where to Find More Information

For more information about Oracle Financial Services and the FSDM, refer to the following documents:

- The *Data Interface Specification (DIS)* identifies the set of business data files that are required for each Oracle solution set and specifies the proper format in which the data is to be provided such that Oracle Financial Services can ingest it.
- The *Administration Guide* explains how the software works, and provides instructions for configuring Oracle Financial Services, its subcomponents, and required third-party software for operation. With respect to the FSDM specifically, it describes the steps by which data is processed and loaded (ingested) into the database.
- The *Financial Services Data Model Reference Guide*, Volume 1, *Business Data*, defines the tables Oracle Financial Services uses to capture and store business data, including reference and transaction data.

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

FSDM Reference Guide, Volume 3: Case Management Data

This chapter provides a brief overview of the purpose, scope, and organization of this document.

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide

Who Should Use this Guide

The *Financial Services Data Model (FSDM) Reference Guide, Volume 3, Case Management Data* is designed for use by Oracle client Investigators and Information Technology (IT) Support Staff, as well as for use by the Oracle Professional Services and Development Teams. Their roles and responsibilities include the following:

- **Investigator:** This user analyzes and dispositions cases within Oracle Financial Services Enterprise Case Management™ (herein referred to as Enterprise Case Management or ECM). An understanding of the data provided in the FSDM can support their ability to manage cases successfully.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the correct form, querying ECM data to support troubleshooting and reporting activities requested by the business, and delivering data to Oracle Financial Services.
- **Oracle Financial Services Professional Services Team and Partners:** This user is responsible for deploying Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services..

Scope of this Guide

This guide describes how the data in the FSDM is organized, how Enterprise Case Management uses the data, and how to achieve specific business outcomes with the data.

How this Guide is Organized

The *Financial Services Data Model Reference Guide*, Volume 3, *Case Management Data* is organized as follows:

- **Chapter 1, *Introduction***, details elements that many of the subject areas share within the FSDM.
- **Chapter 2, *Case Management Configuration Data***, details how Enterprise Case Management configuration related data is stored in the FSDM.
- **Chapter 3, *Case Management Investigation Data***, details how case management related data is stored in the FSDM.
- **Chapter 4, *Account Data***, details how account-related data associated with the case is stored in the FSDM.
- **Chapter 5, *Customer Data***, details how customer-related data associated with the case is stored in the FSDM.
- **Chapter 6, *Enterprise Data***, details how enterprise-related data associated with the case is stored in the FSDM.
- **Chapter 7, *Transaction Data***, details how transaction-related data associated with the case is stored in the FSDM.
- **Chapter 8, *Trade Finance Data***, details how trade finance-related data associated with the case is stored in the FSDM.
- **Appendix A, “Common Tables,”** details how data used by the Enterprise Case Management subject area may be stored in the Behavior Detection and Business Data subject areas of the Oracle Financial Services FSDM.

Where to Find More Information

For more information about Oracle Financial Services and the FSDM, refer to the following documents:

- The *Administration Guide* explains how the software works, and provides instructions for configuring Oracle Financial Services, its subcomponents, and required third-party software for operation. With respect to the FSDM specifically, it describes the steps by which data is processed and loaded (ingested) into the database.
- The *FSDM*, Volume 1, *Business Data*, defines the tables Oracle Financial Services uses to capture and store business data, including reference and transaction data.
- The *FSDM*, Volume 2, *Oracle Financial Services Data*, defines the tables Oracle uses to capture and store behavior detection and Behavior Detection data (applicable if your firm has implemented Oracle Financial Services Behavior Detection).
- The *Data Interface Specification (DIS)* identifies the set of business data files that are required for each Oracle solution set and specifies the proper format in which the data is to be provided such that it can be ingested.

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

This guide provides supporting information for the Oracle Financial Services Behavior Detection Applications Pack (OFS BD) Installation Guide and includes the following topics:

- About this Guide
- Who Should Use this Guide
- Prerequisites
- How this Guide is Organized
- Where To Find More Information

About this Guide

This guide provides instructions for installing and configuring the Platform system, subsystem components, and the related third-party software needed to operate the system. You can find the latest copy of this document in OTN Library which includes all the recent additions/revisions (if any) done till date.

Before you begin the installation, ensure that you have an access to the Oracle Support Portal with the required login credentials to quickly notify us of any issues at any stage. You can obtain the login credentials by contacting Oracle Support.

Who Should Use this Guide

Oracle Financial Services Behavior Detection Pack Installation Guide is intended for administrators and implementation consultants who are responsible for installing and maintaining the Applications Pack components. Their roles and responsibilities include the following:

- **Platform Installer:** This user installs and configures Platform and the client-specific solution sets at a deployment site. The Platform Installer also installs upgrades, additional solution sets, and requires access to deployment-specific configuration information (for example, machine names and port numbers).
- **System Administrator:** This user configures, maintains, and adjusts the system and is usually an employee of a specific Platform client. The System Administrator maintains user accounts and roles, archives data, loads data feeds, and updates the News and Notes information available to users through the Kiosk page.

Prerequisites

Following are the expected preparations from the administrator before starting the actual installation.

The document assumes that you have experience in installing Enterprise components and basic knowledge about the following are recommended:

- Oracle Financial Services Behavior Detection pack components
- OFSAA Architecture
- UNIX Commands
- Database Concepts
- Web Server/Web Application Server

How this Guide is Organized

The *Oracle Financial Services Behavior Detection Pack Installation Guide* includes the following chapters and appendices:

- Chapter 1, *About OFSAA and OFSAA Applications Packs*, provides complete details about Behavior Detection (BD) Applications Pack..
- Chapter 2, *Understanding OFS BD Pack Installation*, explains the installation process, describes the configuration details, and describes the GUI and SILENT installations.
- Chapter 3, *Preparing for Installation*, provides necessary information to review before installing the Oracle Financial Services Behavior Detection (OFS BD) Applications Pack.
- Chapter 4, *Installing OFS BD Pack*, describes the steps to be followed to install the OFS BD pack depending on the offline and online modes of installation.
- Chapter 5, *Upgrading the OFS BD Application Pack*, describes the steps to be followed to upgradethe OFS BD pack and the post-installation steps.
- Chapter 6, *Post Installation Configuration*, explains how to create and deploy the Applications Pack Web Archive, configure and deploy Scenario Wizard and Services, install and configure the Scenario Manager application, deploy the Analytic Reports and Threshold Analyzer, configure the Resource Reference, Web Application Server, OFSDF, Big Data Processing, and load new or modified scenarios.
- Chapter 7, *Post Deployment Configuration*, provides detailed information about the Post Deployment Configuration and lists the various configurations to be completed before you use the OFSAA Applications.
- Appendix A, *Configuring Web Server*, provides detailed information about how to configure OFSBD on various web servers, including WebSphere, WebLogic, and Apache Tomcat.
- Appendix B, *Configuring Resource Reference in Web Application Servers*, provides detailed information about how to configure Resource Reference on various web servers, including WebSphere, WebLogic, and Apache Tomcat.
- Appendix C, *Creating and Deploying EAR/ WAR File*, provides detailed information about how to create and deploy .ear and .war files on various web servers, including WebSphere, WebLogic, and Apache Tomcat.
- Appendix D, *Starting / Stopping Infrastructure Services*, provides details about how to start and stop Infrastructure services.
- Appendix E, *Starting / Stopping Infrastructure Services*, details the steps to be performed to access OFSAA Application.

- Appendix F, *Cloning OFSAA Instance*, explains how to find information about setting up OFSAA instances that are exact copies of the current OFSAA instance.
- Appendix G, *OFSAA Landing Page*, describes the OFSAA Common Landing page and how to enable applications within that page.
- Appendix H, *Additional Configuration*, gives detailed information about the Additional Configuration regarding OFSAA Installation.
- Appendix I, *Patching OFSAA Infrastructure Installation* describes where to find information on the latest OFSAA software patchsets.
- Appendix J, *Grants for Atomic/ Config Schema*, discusses the various grants required for the CONFIG, and ATOMIC schemas.
- Appendix K, *Configuring Applications Pack XML Files*, describes configuration of OFS_BD_PACK.xml and OFS_BD_SCHEMA_IN.xml files.
- Appendix L, *Configuring OFSAAI_InstallConfig.xml File*, describes the OFSAAI_InstallConfig.xml file.
- Appendix M, *Migration for Excel Upload*, provides detailed instructions for migrating using the Excel Upload feature.
- Appendix N, *JDBC Jar Files*, describes where to find the ojdbc<version>.jar file which should be copied based on Database & Java version.
- Appendix O, *Upgrading an Existing OFSAA 8.0.x Java 7 Instance to Java 8*, explains the configurations required to upgrade an existing OFSAA 8.0.x Java 7 instance to Java 8.n.
- Appendix P, *Removing OFSAA*, gives detailed information about how to uninstall and remove OFSAA.
- Appendix Q, *Tunable Database Parameters*, contains the Tunable Database Parameters.
- Appendix R, *FAQs and Error Dictionary*, contains resolution to the frequently asked questions and error codes noticed during OFSAAI installation.

Where To Find More Information

For more information about Oracle Financial Services Behavior Detection, refer to the following documents:

- OFSAAI Related Documents
 - Oracle Financial Services Advanced Analytical Applications Infrastructure Applications Pack Installation and Configuration Guide
 - Oracle Financial Services Analytical Applications Infrastructure Environment Check Utility Guide
 - Oracle Financial Services Analytical Applications Infrastructure Administration Guide
 - Oracle Financial Services Analytical Applications Infrastructure User Guide
- OFS BD Application Related Documents
 - Oracle Financial Services Behavior Detection Administration Guide
 - Oracle Financial Services Scenario Manager User Guide
 - Oracle Financial Services Behavior Detection Configuration Guide
 - Oracle Financial Services Know Your Customer Administration Guide
 - Oracle Financial Services Currency Transaction Reporting Administration Guide
 - Oracle Financial Services Scenario Wizard Configuration Guide
 - Oracle Financial Services Know Your Customer Risk Assessment Guide
 - Oracle Financial Services Administration Tools User Guide
 - Oracle Financial Services FATCA Administration and Configuration Guide
 - Oracle Financial Services FATCA Assessment Guide
 - Oracle Financial Services FATCA RR User Guide
 - Oracle Financial Services FATCA RR Administration and Configuration Guide
 - Oracle Financial Services Alert Management User Guide
 - Oracle Financial Services Enterprise Case Management User Guide
 - Oracle Financial Services Common Reporting Standard User Guide
 - Oracle Financial Services Common Reporting Standard Administration Configuration Guide
 - Oracle Financial Services Behavior Detection Release Notes

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

This guide provides supporting information for the Oracle Financial Services Behavior Detection (OFS BD) Applications Pack Release.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

About this Guide

This guide identifies known issues, software corrections, and supplemental installation instructions associated with the current release for the Oracle Financial Services Behavior Detection Application Pack, which includes the following Oracle solution sets:

- Oracle Financial Services Alert Management
- Oracle Financial Services FCCM Analytics
- Oracle Financial Services Anti Money Laundering
- Oracle Financial Services Behavior Detection
- Oracle Financial Services Broker Compliance
- Oracle Financial Services Common Reporting Standards
- Oracle Financial Services Currency Transaction Reporting
- Oracle Financial Services Energy and Commodity Trading Compliance
- Oracle Financial Services Enterprise Case Management
- Oracle Financial Services FATCA Management
- Oracle Financial Services Enterprise Fraud Management
- Oracle Financial Services Know Your Customer
- Oracle Financial Services Personal Trading Approval
- Oracle Financial Services Trading Compliance
- Oracle Financial Services Trade Blotter

Who Should Use this Guide

This document is intended for users of the Oracle Financial Services Behavior Detection Application Pack, specifically those interested in a broad overview of the new features in this release. Additionally, this document is provided for those who want to know specifically which issues or change requests from the previous release have been resolved, which scenarios have been impacted by any changes, and which issues remain.

How this Guide is Organized

This guide contains the following chapters:

- Chapter 1, *Release Highlights*, provides an overview of the new features, enhancements, and other improvements made to the current Oracle release.
- Chapter 2, *Introduction*, provides an overview of Oracle Financial Services Analytical Applications (OFSAA) and Oracle Financial Services Behavior Detection applications and solution sets.
- Chapter 3, *Oracle Financial Services Analytical Applications Infrastructure*, provides new features in the OFSAA release. It also provides a list of all OFSAA issues reported by external organizations that were resolved in the latest Oracle release, by subsystem, as well as a list of all Limitations in this OFSAA release.
- Chapter 4, *Oracle Financial Services Behavior Detection*, provides new features in the OFSBD release. It also provides a list of all OFSBD issues reported by external organizations that were resolved in the latest Oracle release, by subsystem, as well as a list of all Limitations in this OFSBD release.
- Chapter 5, *Hardware/Software Tech Stack Details*, describes where to find the latest information pertaining to hardware/software combinations required for this release.
- Chapter 6, *Third-Party Software Tools*, describes where to find the latest information pertaining to third-party software required for this release.

Where to Find More Information

For more information about Oracle Financial Services products, refer to the following documents:

- Oracle Financial Services Behavior Detection Applications Pack Installation Guide
- Administration Tools User Guide
- Alert Management User Guide
- Analytics User Guide
- Anti-Money Laundering Technical Scenario Description
- Behavior Detection Administration Guide
- Behavior Detection Configuration Guide
- Behavior Detection Data Interface Specification
- Broker Compliance Technical Scenario Description
- Common Reporting Standard Administration and Configuration Guide

- Common Reporting Standard User Guide
- Currency Transaction Reporting Administration and Configuration Guide
- Currency Transaction Reporting Technical Scenario Description
- Currency Transaction Reporting User Guide
- Energy and Commodity Trading Compliance Technical Scenario Description
- Enterprise Case Management User Guide
- FATCA Management Administration and Configuration Guide
- FATCA Management Assessment Guide
- Financial Services Data Model Reference Guide Volume 1: Business Data
- Financial Services Data Model Reference Guide Volume 2: Oracle Financial Services Data
- Financial Services Data Model Reference Guide Volume 3: Case Management Data
- Fraud Technical Scenario Description
- Glossary of Financial Crimes and Compliance Management Products
- Know Your Customer Administration Guide
- Know Your Customer Data Model Reference Guide
- Know Your Customer Risk Assessment Guide
- Know Your Customer Service Guide
- Personal Trading Approval User Guide
- Scenario Manager User Guide
- Scenario Wizard Configuration Guide
- Security Guide
- Services Guide
- Trading Compliance Technical Scenario Description
- Oracle Financial Services Analytical Applications 8.0.4.0.0 Technology Matrix

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about Oracle Financial Services and our complete product line, visit our web site at www.oracle.com/financialservices.

This guide explains how to use all of the features and functionality of the Scenario Manager application (referred to herein as the Scenario Manager).

This chapter contains the following sections:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Scenario Manager User Guide*, Release is designed for use by the Data Miners. The Data Miner is responsible for adjusting the pattern logic or thresholds of existing scenarios and employing data mining techniques to define new patterns and scenarios. This includes both mining data to detect new scenarios and mining data to identify patterns that indicate known scenarios.

Scope of this Guide

This guide defines the features, functionality, and step-by-step procedures for features within the Scenario Manager including its tools:

- DataSet Editor
- Sequence Scenario Editor
- Rule Scenario Editor
- Link Analysis
- Job Editors
- Threshold Manager
- Augmentation

How this Guide is Organized

The *Scenario Manager User Guide*, contains the following chapters:

- Chapter 2, *About Scenario Manager*, defines the features and functionality of the Scenario Manager.
- Chapter 3, *Common Features*, defines the features, functionality, and processes that are common throughout the Scenario Manager.
- Chapter 4, *DataSet Editor*, defines the DataSet Editor features and functionality within the Scenario Manager.
- Chapter 5, *Sequence Scenario Editor*, defines the Sequence Scenario Editor features and functionality within the Scenario Manager.
- Chapter 7, *Rule Scenario Editor*, defines the Rule Scenario Editor features and functionality within the Scenario Manager.
- Chapter 6, *Link Analysis*, defines the Link Analysis feature and functionality of each of the dataset editors within the Scenario Manager.
- Chapter 8, *Threshold Manager*, defines the Threshold Manager features and functionality within the Scenario Manager.
- Chapter 9, *Augmentation*, defines the augmentation tool features and functionality within the Scenario Manager.
- Chapter 10, *Job Editors*, defines the Job Editors' features and functionality within the Scenario Manager.
- Appendix A, *Scenario Design Guidelines*, describes technical guidelines for the design of scenarios and their components.
- Appendix B, *Naming Conventions*, provides naming conventions for creating datasets and scenario components.
- Appendix C, *Scenario Manager to User Interface Mapping*, provides an example of mapping elements of a scenario and pattern roles to the Web Application User Interface (UI).
- The *Index* provides an alphabetized cross-reference list that helps you locate information quickly.

Where to Find More Information

For more information about Oracle Financial Services products, refer to the following documents:

- *Administration Guide*
- *Installation Guide*
- *Alert Management User Guide*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about Oracle Financial Services and our complete product line, visit our web site at www.oracle.com/financialservices.

This document provides security information associated with the Oracle Financial Services Behavior Detection Framework.

This chapter focuses on the following topics:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information
- To find more information about FCCM and our complete product line, visit our web site at www.oracle.com/financialservices.

Who Should Use this Guide

The *Oracle Financial Services Behavior Detection Framework Security Guide* is designed for use by Financial Crime and Compliance Management (FCCM) System Administrators. This user configures, maintains, and adjusts the system and is usually an employee of a specific FCCM product client. The System Administrator maintains user accounts and roles, archives data, and loads data feeds.

Scope of this Guide

This guide provides instructions for installing and configuring the FCCM product system, subsystem components, and the related third-party software needed to operate the system.

How this Guide is Organized

This guide contains the following chapters:

- Chapter 1, *About Security and Guidelines*, provides a brief overview of the security procedures.
- Chapter 2, *Security Checklist*, provides examples of recommended security policies.
- Chapter 3, *Database Security*, provides steps detailing how to secure your FCCM product database.
- Chapter 4, *Web Services Subsystem Security*, provides steps detailing how to secure the Investigation Management subsystem.
- Chapter 5, *Password Management*, provides information about the Password Manager Utility and how to establish an effective password policy.
- Chapter 6, *Ingestion Manager Subsystem Security*, provides security information about the Ingestion Manager subsystem directory.
- Chapter 7, *Third-Party Applications*, provides security information about third-party applications used by the FCCM application.

Where to Find More Information

For more information about the Platform Behavior Detection Platform, refer to the following documents:

- *Administration Guide*: Explains how the software works and provides instructions for configuring Oracle Financial Services Behavior Detection Framework (OFS BDF), its subcomponents, and required third-party software for operation.
- *Scenario Manager User Guide*: Provides instructions on how to use the Scenario Manager.
- *Configuration Guide*: Provides instructions on how to configure the FCCM product user interface.
- *Data Interface Specification (DIS)*: Identifies the proper format for all data that is ingested into the system.
- *FSDM Vol. 1, FSDM Vol. 2, and FSDM Vol. 3*: Provide a visual representation of the data relationships within the physical data model.

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about FCCM and our complete product line, visit our web site at www.oracle.com/financialservices.

Part 2: Front-End Documents

This guide explains the concepts of Oracle Financial Services Alert Management and provides step-by-step instructions for navigating the Oracle Financial Services web pages, analyzing alerts, acting on alerts, and researching the business information.

This chapter focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Alert Management User Guide* is designed for the following users:

- **Analyst:** This user works on the alerts within the application frequently. This user's specific role (that is, Analyst I or Analyst II) determines what this user can see and do within the application.
- **Supervisor:** This user works on alerts within the application on a daily basis and is typically a higher level Analyst or Compliance Officer.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts; however, this user can view many areas within the application and can perform only a limited set of actions.
- **Auditor:** This user has broad viewing rights for alerts within the application; however, this user can perform a limited set of actions based on the user's role (that is, Internal Auditor or External Auditor).

How this Guide is Organized

The *Alert Management User Guide*, includes the following chapters:

- Chapter 1, *Overview of FCCM*, provides an overview of Oracle Financial Services Financial Crimes and Compliance Management, how it works, and what it does.
- Chapter 2, *About Alert Management*, provides an overview of the Alert Management application, how it works, and what it does.
- Chapter 3, *Getting Started*, includes instructions on how to configure your system, access Alert Management application, and exit the application.
- Chapter 4, *Managing Alerts*, explains the Alerts workflow, how to search for business data and create alerts, and the actions you can take on alerts.
- Chapter 5, *Managing Suppression Rules*, provides instructions for managing suppression rules.
- Chapter 6, *Managing Trusted Pairs*, provides instructions for managing trusted pairs.
- Chapter 7, *Managing Trade Blotter*, provides instructions on reviewing trades, primarily for suitability issues.
- Chapter 8, *Managing Controlling Customers*, describes how to view existing or historical data, update certain components of the controlling customer, and delete existing controlling customers.
- Chapter 9, *Managing Security Restrictions*, explains securities restriction features providing a way to search for existing trading restrictions on different securities based on user-specified search parameters.
- Chapter 10, *Researching Business Data*, describes how to use the Oracle Financial Services Research workflow to search for and inquire about a specific focus type and its related information.
- Chapter 11, *Managing Compliance Regulatory Reporting*, explains the high-level information on Compliance Regulatory Reporting.
- Chapter 12, *Managing Watch List Management*, describes the Oracle Financial Services Watch List Management feature.
- Chapter 13, *Setting User Preferences*, explains how to setup Oracle Financial Services Alert Management and Enterprise Case Management preferences.
- Chapter 14, *Oracle Financial Services Crime and Compliance Management Analytics*, describes the Interactive Analytic reports available in Oracle Financial Services.
- Appendix A, *User Privileges*, provides complete information on the user roles and action they can perform.
- Appendix B, *Alert Components and Tables*, provides the additional information on various components and tables of Alert Management.
- Appendix D, *Business Tabs*, identifies the possible business tab pages that Oracle Financial Services application displays for a specific scenario class and focus type.
- Appendix E, *Using Alert Management Web Pages*, explains common elements of the interface.
- Appendix F, *Message Pages*, explains error and status pages that are not directly related to the business function of the application.
- Appendix G, *Security within Oracle Financial Services Alert Management*, explains how Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) security is used

- Appendix H, *Calculating Risk*, describes how Oracle Financial Services Alert Management uses risk calculations as part of managing sensitivity when detecting behaviors of interest.
- Appendix I, *Trade Blotter List Component Matrix*, lists trade blotter components in the Oracle Financial Services Alert Management application.
- The *Index* provides an alphabetized cross-reference list that helps you to locate information quickly

Where to Find More Information

For more information about Alert Management, refer to the following documents:

- *Administration Guide*
- *Administration Tools User Guide*
- *Configuration Guide*
- *Data Interface Specification (DIS)*
- *FSDM and Data Model Reference Guides*
- *Scenario Manager User Guide*
- *Scenario Wizard Configuration Guide*
- *Installation Guide*
- *Anti Money Laundering Technical Scenario Descriptions*
- *Trading Compliance Technical Scenario Descriptions*
- *Fraud Technical Scenario Descriptions*
- *Broker Compliance Technical Scenario Descriptions*
- *Energy and Commodity Trading Technical Scenario Descriptions*
- *Glossary*
- *Release Notes/ Read me*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about Oracle Financial Services and our complete product line, visit our Web site www.oracle.com/financialservices.

Enterprise Case Management User Guide

This guide explains the concepts of Enterprise Case Management and provides step-by-step instructions for navigating the web pages, analyzing cases, acting on cases, researching business information.

This chapter focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Enterprise Case Management Documentation Overview Guide* is designed for the following users:

- **Case Initiator:** This user manually creates cases for AML/Fraud cases types.
- **Case Analyst:** This user works on the cases within the application frequently. This user's specific role (that is, Case Analyst I or Case Analyst II) determines what this user can see and do within the application.
- **Case Supervisor:** This user works on cases within the application on a daily basis and is typically a higher level Analyst or Compliance Officer.
- **Case Executive:** This user may not be involved in the day-to-day analysis of cases; however, this user can view many areas within the application and can perform only a limited set of actions.
- **Case Auditor:** This user has broad viewing rights for cases within the application; however, this user can perform a limited set of actions based on the user's role (that is, Case Internal Auditor or Case External Auditor).
- **Case Viewer:** This user has specific viewing rights to the cases. This user's specific role (that is, Case Viewer I or Case Viewer II) determines what this user can see within the application.
- **KYC Analyst:** This user works on Know Your Customer (KYC) cases within the application on a daily basis and performs actions defined for analyst user role.
- **KYC Supervisor:** This user works on Know Your Customer (KYC) cases within the application on a daily basis and performs actions defined for supervisor user role.
- **Relationship Manager:** This user can view all the Know Your Customer (KYC) assessments that are in Hold statuses.
- **FATCA Analyst:** This user can view and analyze the (Foreign Account Tax Compliance Act) FATCA Assessments, promote an Assessment to a FATCA Case, view and analyze a FATCA Case, and view and add Withholding Transactions.

- **FATCA Supervisor:** This user can view and analyze the (Foreign Account Tax Compliance Act) FATCA Assessments, promote an Assessment to a FATCA Case, view and analyze a FATCA Case, and view and add Withholding Transactions.
- **FATCA Administrator:** This user is responsible for managing the static data used in FATCA rules, creating users, mapping users to user groups, and configuring the various parameters used in FATCA.
- **FATCA Auditor:** This user is responsible for auditing the FATCA Assessments, FATCA Cases and Withholding Transactions. This user can access all the modules in FATCA Management solution and will have a *View Only* access.

How this Guide is Organized

The *Enterprise Case Management User Guide*, includes the following chapters:

- Chapter 1, *Overview of FCCM*, provides an overview of Oracle Financial Services Financial Crimes and Compliance Management, how it works, and what it does.
- Chapter 2, *About Enterprise Case Management*, provides an overview of Enterprise Case Management application, how it works, and what it does.
- Chapter 3, *Getting Started*, includes instructions on how to configure your system, access Enterprise Case Management application, and exit the application.
- Chapter 4, *About Enterprise Case Management' Web Pages*, explains common elements of the interface.
- Chapter 5, *Investigating Cases*, explains the AML/Fraud case type workflows.
- Chapter 6, *Investigating KYC Assessments and Cases*, explains the KYC Assessments and KYC Case type workflows.
- Chapter 7, *Investigating FATCA Assessments and Cases*, explains the FATCA Assessments, FATCA Cases, and Withholding Transactions workflows.
- Chapter 8, *Working with Compliance Regulatory Reporting*, explains how Compliance Regulatory Reporting is integrated with the application and allows users to generate reports with information relevant to the investigation.
- Chapter 9, *Generating Interactive Analytic Reports*, describes the Interactive Analytic reports available in Enterprise Case Management.
- Chapter 10, *Setting User Preferences*, explains how to setup Enterprise Case Management preferences.
- Appendix A, *Message Pages* explains error and status pages that are not directly related to the business function of the application.
- The *Index*, provides an alphabetized cross-reference list that helps you to locate information quickly.

Where to Find More Information

For more information about Enterprise Case Management, refer to the following documents:

- *Administration Guide*
- *Configuration Guide*
- *Alert Management User Guide*
- *Data Interface Specification (DIS)*
- *Installation Guide - Stage 3*
- *Release Notes*
- *Anti-Money Laundering Technical Scenario Descriptions*
- *Fraud Technical Scenario Descriptions*
- *KYC Risk Assessment Guide*
- *FATCA Administration and Configuration Guide*
- *FATCA Assessment Guide*
- *FATCA Data Interface Specification*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about Oracle Financial Services and our complete product line, visit our Web site www.oracle.com/financialservices.

Personal Trading Approval User Guide

The *Personal Trading Approval User Guide* explains the concepts of Personal Trading Approval and provides step-by-step instructions for navigating through the application.

This chapter discusses the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Personal Trading Approval User Guide* is designed for the following users of the Personal Trading Approval application.

- Employee
- Control Room Supervisor
- Control Room Analyst
- IP Manager Supervisor
- IP Manager

How this Guide is Organized

The *Oracle Financial Services Personal Trading Approval User Guide* includes the following topics:

- Chapter 1, About Personal Trading Approval,, describes the Personal Trading Approval application, its workflow, and user roles and actions.
- Chapter 2, Getting Started,, explains how to access and login to the application.
- Chapter 3, Account Approval, provides information about navigating through the User Interface and performing various actions in the Account Approval Request section.
- Chapter 4, Pre-Trade Approval,, provides information about navigating through the User Interface and performing various actions in the Pre-Trade Approval section.
- Chapter 5, Attestation, provides information about navigating through the User Interface and performing various actions in the Attestation section.

- Chapter 6, *Reports* provides information about the various reports used by the Personal Trading Approval application.

Where to Find More Information

For more information on Oracle Financial Services, refer to the following documents:

- *Administration Guide*
- *Configuration Guide*
- *Installation Guide*
- *Release Notes*

To find additional information about how Oracle Financial Services solves real business problems, see our Web site at www.oracle.com/financialservices.

Glossary of Financial Crime and Compliance Management Products

This chapter provides a high-level description of the *Glossary of Financial Crime and Compliance Management Products*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide

About this Guide

This guide is used as a reference for the terms used in the Oracle Financial Services Financial Crime and Compliance Management Products. The Glossary explains terms and acronyms according to their use in the Oracle Financial Services Financial Crime and Compliance Management Products application.

Who Should Use this Guide

The *Oracle Financial Services Glossary of Financial Crime and Compliance Management Products* is designed for users, that includes both Oracle as well as client personnel.

This chapter focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

The *Services Guide* is designed for use by Oracle Financial Services System Integrators. Their roles and responsibilities, as they work with the application include the following:

- **Systems Integrator:** Integrates information with external applications. The Integrator uses the interfaces that this guide describes, to access and pass information between applications.

How this Guide is Organized

The *Services Guide* includes the following chapters:

- Chapter 1, *Services Overview*, provides an overview of the Oracle Financial Services Behavior Detection Framework (OFSBDF) Web services interfaces.
- Chapter 2, *Web Services*, describes the Web services interfaces for integrating OFSBDF Alert Management data with other systems.
- Appendix A, *Alert Management Services XML Specifications*, provides the XML representation for OFSBDF Alert Management services specifications.
- Appendix B, *Watch List Service XML Specifications*, provides the XML representation for OFSBDF Scan Watch List Service specifications.
- Appendix C, *Services Content Definitions*, provides descriptions of the XML elements used to define the OFSBDF services.
- Appendix D, *Sample Services Requests and Responses*, provides samples of OFSBDF post services' requests and responses.
- Appendix E, *SSL (HTTPS) Support for Web Services*, explains configuring and using SSL(HTTPS) ports for accessing web services.

Where to Find More Information

For more information about OFSBDF, refer to the following documents:

- *Scenario Manager User Guide*
- *Installation Guide*
- *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration*
- *Administration Tools User Guide*
- *Administration Guide*
- *Configuration Guide*
- *Alert Management User Guide and Enterprise Case Management User Guide*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about Oracle Financial Services and our complete product line, visit our web site at www.oracle.com/financialservices.

Technical Scenario Description - Anti-Money Laundering Solution

This chapter provides the high-level description of the *Anti-Money Laundering (AML) Solution Technical Scenario Description (TSD)*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized

About this Guide

The *AML Solution TSD* uses advanced behavior detection techniques to identify behaviors of interest or scenarios, which are indicative of potentially suspicious behavior and possible money laundering activities. The product enables comprehensive monitoring of transactions, accounts, and customers across business lines and products. Specifically, it facilitates the detection of suspicious activity and proactive investigation and the reporting of money laundering activities. This document outlines the scenarios in the Oracle Financial Services AML solution sets.

The major scenario coverage areas are organized as follows:

- **Scenario Areas:** A logical presentation of scenarios in the scenario description document.
- **Scenario Group:** A set of one or more scenarios that pertain to the same behavior of interest. Each scenario within a scenario group contains different business logic that is further refined through its specific patterns and tunable parameters.
- **Scenario:** A behavior of interest. Each scenario pertains to one focus type and underlying pattern and tunable thresholds.

Who Should Use this Guide

The *Anti Money Laundering Technical Scenario Description*, is designed for use by Oracle Financial Services and client personnel. Their roles and responsibilities include the following:

- **Analyst:** This user works in the application frequently. This user's specific role (Analyst I, Analyst II, or Analyst III) determines what this user can see and do within the application.
- **Auditor:** This user has broad viewing rights within the application, but can perform a limited set of actions based upon the user's role (Internal Auditor or External Auditor).
- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services Behavior Detection Platform generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.
- **Data Miner:** This user accesses the Administration Tools to modify the threshold values used by patterns to detect matches in Firm data.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts. This user can view many areas within the application but can perform only a limited set of actions.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the form that Oracle Financial Services requires, and delivering that data to Oracle Financial Services.
- **Oracle Financial Services Administrator:** This user accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. This user is typically an employee of a specific Oracle Financial Services customer.
- **Oracle Financial Services Development Team:** This user is responsible for developing the Oracle Financial Services scenarios and the user interface, which are based entirely on the data that the TSDs and FSDM provide.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Supervisor:** This user works in the application on a daily basis and is typically a higher level Analyst or Compliance Officer.

How this Guide is Organized

The *Oracle Financial Services Behavior Detection Platform Anti-Money Laundering Solution Technical Scenario Description* includes the following topics:

- Chapter 1, *Introduction*, describes the classes that are explained in the guide.
- Chapter 2, *How to Read the Technical Scenario Descriptions*, describes the layout (a description of the headings) of each technical scenario description, explains how to read the information, and provides notes on styles.
- Chapter 3, *High Risk Geographies and Entities*, describes scenarios related to financial institutions typically identifying certain geographies as high risk due to the increased risk for money laundering. Institutions also maintain watch lists or hot lists of entities that, based on previous experience, warrant enhanced scrutiny.
- Chapter 4, *Hidden Relationships*, describes scenarios related to scenarios addressing the detection of activity between accounts, customers, correspondents, and other entities to reveal previously unknown relationships that could be indicative of efforts to launder funds.
- Chapter 5, *Anomalies in Behavior*, describes scenarios addressing sudden, significant changes in transaction activity that could be indicative of money laundering or fraud. They also address the rapid movement of funds into and out of an account, or in and out of the institution through multiple accounts, as well as rapid escalation in a previously dormant account's activity.
- Chapter 6, *Other Money Laundering Behaviors*, describes scenarios addressing other types of activities that are considered potentially suspicious or indicative of money laundering, such as attempts to structure, patterns of cash transactions, and so forth.
- Chapter 7, *Insurance Scenarios*, describes scenarios monitoring potential money laundering activities through insurance products. They detect instances where customers initiate policies with *dirty* money and subsequently receive *clean* funds in return through policy loans, cancellation, surrender, or premium overpayment.
- Chapter 8, *ATM, Debit, Bank Card, and Credit Scenarios*, describes fraud scenarios in detail. These scenarios have two focus types—Account focus and Customer focus.
- Chapter 9, *Institutional Anti-Money Laundering Scenarios*, describes scenarios in a group for different types of changes in account behavior based on customer or account profiles. While these types of changes can be of interest, further review is typically required to distinguish between changes resulting from money laundering or fraud schemes such as account takeover or identity theft.

Technical Scenario Description - Broker Compliance

This chapter provides the high-level description of the *Oracle Financial Services Behavior Detection Platform Broker Compliance (BC) Solution Technical Scenario Description (TSD)*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized

About this Guide

The Oracle Financial Services Behavior Detection Platform Broker Compliance (BC) Solution uses advanced behavior detection techniques to identify behaviors of interest, or scenarios, which are indicative of potentially suspicious behavior. The product enables comprehensive monitoring of transactions, accounts, customers across business lines and products, and facilitates the detection of suspicious activity and proactive investigation. This document outlines the scenarios in the Oracle Financial Services BC solution set.

The major scenario coverage areas are organized as follows:

- **Scenario Areas:** A logical presentation of scenarios in the scenario description document.
- **Scenario Group:** A set of one or more scenarios that pertain to the same behavior of interest. Each scenario within a scenario group contains different business logic that is further refined through its specific patterns and tunable parameters.
- **Scenario:** A behavior of interest. Each scenario pertains to one focus type, an underlying pattern, and to tunable thresholds.

Who Should Use this Guide

The *Oracle Financial Services Broker Compliance Technical Scenario Description Guide* is designed for use by all users of the product. Their roles and responsibilities include the following:

- **Analyst:** This user works in the application frequently. This user's specific role (Analyst I, Analyst II, or Analyst III) determines what this user can see and do within the application.
- **Auditor:** This user has broad viewing rights within the application but can perform a limited set of actions based upon the user's role (Internal Auditor or External Auditor).
- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services Behavior Detection Platform generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.
- **Data Miner:** This user accesses the Administration Tools to modify the threshold values used by patterns to detect matches in a Firm's data.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts. This user can view many areas within the application but can only perform a limited set of actions.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the form Oracle Financial Services requires, and delivering that data to Oracle Financial Services.
- **Oracle Financial Services Administrator:** This user accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. This user is typically an employee of a specific Oracle Financial Services customer.
- **Oracle Financial Services Development Team:** This user is responsible for developing the Oracle Financial Services scenarios and the user interface, which are based entirely on the data that the TSDs and FSDM provide.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Supervisor:** This user works in the application on a daily basis and is typically a higher level Analyst or Compliance Officer.

How this Guide is Organized

The *Broker Compliance Solution Technical Scenario Description* includes the following topics:

- Chapter 1, *Introduction*, describes the classes that are explained in the guide.
- Chapter 2, *How to Read the Technical Scenario Descriptions*, describes the layout (a description of the headings) of each technical scenario description, explains how to read the information, and provides notes on styles.
- Chapter 3, *Customer Risk and Suitability*, identifies activities or situations in customer accounts that involve either a significant amount of risk—and therefore may be unsuitable for the customer—or may violate trading rules set by the exchanges or regulators. This class covers behaviors initiated either directly by customers or by registered representatives who serve customer accounts.
- Chapter 4, *Mutual Funds*, identifies trades in mutual fund securities that may violate regulatory trading guidelines, Commission policies, or trades which are unsuitable for a particular customer.
- Chapter 5, *Employee Trading*, identifies activities performed by employees that may violate regulatory conduct rules or may be prohibited by firm policies.
- Chapter 6, *Investment Advisor*, identifies instances in which an investment advisor may be managing client accounts in a manner that is unsuitable for their customers, giving preferential treatment to particular customers, or manipulating transactions between accounts.

Technical Scenario Description - Currency Transaction Reporting

This chapter provides the high-level description of the *Oracle Financial Services Behavior Detection Platform Currency Transaction Reporting (CTR) Solution Technical Scenario Description (TSD)*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized

About this Guide

The Oracle Financial Services Behavior Detection Platform Currency Transaction Reporting (CTR) Solution uses advanced behavior detection techniques to identify behaviors of interest, or scenarios, which are indicative of potentially suspicious behavior. The product enables comprehensive monitoring of transactions, accounts, customers across business lines and products, and facilitates the detection of suspicious activity and proactive investigation. This document outlines the scenarios in the Oracle Financial Services CTR solution set.

The CTR scenarios are organized into one class that covers behaviors or situations which may warrant filing a Currency transaction Report in accordance with FinCEN requirements. Future CTR scenario classes may cover additional behaviors or situations.

The major scenario coverage areas are organized as follows:

- **Scenario Areas:** A logical presentation of scenarios in the scenario description document.
- **Scenario Group:** A set of one or more scenarios that pertain to the same behavior of interest. Each scenario within a scenario group contains different business logic that is further refined through its specific patterns and tunable parameters.
- **Scenario:** A behavior of interest. Each scenario pertains to one focus type, an underlying pattern, and to tunable thresholds.

Who Should Use this Guide

The *Currency Transaction Reporting Technical Scenario Description Guide* is designed for use by all users of the product. Their roles and responsibilities include the following:

- **Analyst:** This user works in the application frequently. This user's specific role (Analyst I, Analyst II, or Analyst III) determines what this user can see and do within the application.
- **Auditor:** This user has broad viewing rights within the application but can perform a limited set of actions based upon the user's role (Internal Auditor or External Auditor).
- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services Behavior Detection Platform generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.
- **Data Miner:** This user accesses the Administration Tools to modify the threshold values used by patterns to detect matches in a Firm's data.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts. This user can view many areas within the application but can only perform a limited set of actions.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the form Oracle Financial Services requires, and delivering that data to Oracle Financial Services.
- **Oracle Financial Services Administrator:** This user accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. This user is typically an employee of a specific Oracle Financial Services customer.
- **Oracle Financial Services Development Team:** This user is responsible for developing the Oracle Financial Services scenarios and the user interface, which are based entirely on the data that the TSDs and FSDM provide.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Supervisor:** This user works in the application on a daily basis and is typically a higher level Analyst or Compliance Officer.

How this Guide is Organized

The *Currency Transaction Reporting Technical Scenario Description Guide* includes the following topics:

- Chapter 1, *Introduction*, describes the classes that are explained in the guide.
- Chapter 2, *How to Read the Technical Scenario Descriptions*, describes the layout (a description of the headings) of each technical scenario description, explains how to read the information, and provides notes on styles.
- Chapter 3, *Currency Transaction Reporting*, identifies activities or situations meeting the requirements for filing a Currency Transaction Report (CTR) for currency transactions of the Oracle client firm. The resulting CTRs are to be prepared for electronic filing in accordance with FinCEN's Electronic Filing Requirements. This class covers behaviors initiated by customers, conductors, or entities using tax identifier numbers.

Technical Scenario Description - Energy and Commodity Trading Compliance

This chapter provides a high-level description of the *Oracle Financial Services Energy and Commodity Trading Compliance (ECTC) Solution Technical Scenario Description (TSD)*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized

About this Guide

The Oracle Energy and Commodity Trading Compliance (ECTC) solution uses advanced behavior detection techniques, or scenarios, to identify potentially problematic behaviors with respect to energy and commodity instrument regulations and quality of customer service. This guide outlines the scenarios included in the Energy and Commodity Trading Compliance solution.

The ECTC scenarios are organized into one class that covers behaviors or situations involving firm's traders making deals in energy and commodity instruments. Future ECTC scenario classes may cover behaviors or situations involving firm's customers.

The major scenario coverage areas are organized as follows:

- **Scenario Areas:** A logical presentation of scenarios in the scenario description document.
- **Scenario Group:** A set of one or more scenarios that pertain to the same behavior of interest. Each scenario within a scenario group contains different business logic that is further refined through its specific patterns and tunable parameters.
- **Scenario:** A behavior of interest. Each scenario pertains to one focus type, an underlying pattern, and to tunable thresholds.

Who Should Use this Guide

The *Energy and Commodity Trading Compliance Technical Scenario Description* is designed for use by all users of the product. Their roles and responsibilities include the following:

- **Analyst:** This user works in the application frequently. This user's specific role (Analyst I, Analyst II, or Analyst III) determines what users can see and do within the application.
- **Auditor:** This user has broad viewing rights within the application, but can perform a limited set of actions based upon the user's role as an Internal Auditor or External Auditor.
- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services Behavior Detection Platform generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.
- **Data Miner:** This user accesses the Administration Tools to modify the threshold values used by patterns to detect matches in a firm's data.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts. This user can view many areas within the application but can perform only a limited set of actions.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the form that Oracle Financial Services requires, and delivering that data to Oracle Financial Services.
- **Oracle Financial Services Administrator:** This user accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. This user is typically an employee of a specific Oracle Financial Services customer.
- **Oracle Financial Services Development Team:** This user is responsible for developing the Oracle Financial Services scenarios and the user interface, which are based entirely on the data that the TSDs and FSDM provide.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Supervisor:** This user works in the application on a daily basis and is typically a higher level Analyst with confidential information held by the Firm on a security.

How this Guide is Organized

The *Energy and Commodity Trading Solution Technical Scenario Description Guide* includes the following topics:

- Chapter 1, *Introduction*, describes the scenarios included in the Energy and Commodity Trading solution.
- Chapter 2, *How to Read the Technical Scenario Descriptions*, describes the layout (a description of the headings) of each technical scenario description, explains how to read the information, and provides notes on styles.
- Chapter 3, *Energy and Commodity Trading*, examines prices and timing of orders and executions by comparing them to market conditions.

Technical Scenario Description - Fraud Detection

This chapter provides the high-level description of the *Oracle Financial Services Fraud Detection Technical Scenario Description*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized

About this Guide

The Oracle Financial Services Fraud Detection Solution uses advanced behavior detection techniques to identify sophisticated frauds such as internal employee fraud, identity theft, account takeover, change of customer registration, and other malicious behaviors that today's *profiling based* solutions cannot detect. This guide outlines the scenarios in the Oracle Financial Services Fraud Detection solution sets.

The Fraud Detection TSD guide describes all complex behaviors across large amounts of current and historical information, and alerts institutions about accounts that may be at risk for fraud, based upon close analysis of this information.

The major scenario coverage areas are organized as follows:

- **Scenario Areas:** A logical presentation of scenarios in the scenario description document.
- **Scenario Group:** A set of one or more scenarios that pertain to the same behavior of interest. Each scenario within a scenario group contains different business logic that is further refined through its specific patterns and tunable parameters.
- **Scenario:** A behavior of interest. Each scenario pertains to one focus type, an underlying pattern, and to tunable thresholds.

Who Should Use this Guide

The *Fraud Technical Scenario Description Guide* is designed for use by all users of the product. Their roles and responsibilities include the following:

- **Analyst:** This user works in the application frequently. This user's specific role (Analyst I, Analyst II, or Analyst III) determines what users can see and do within the application.
- **Auditor:** This user has broad viewing rights within the application, but can perform a limited set of actions based upon the user's role as an Internal Auditor or External Auditor.
- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services Behavior Detection Platform generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.
- **Data Miner:** This user accesses the Administration Tools to modify the threshold values used by patterns to detect matches in a firm's data.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts. This user can view many areas within the application but can perform only a limited set of actions.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the form that Oracle Financial Services requires, and delivering that data to Oracle Financial Services.
- **Oracle Financial Services Administrator:** This user accesses the Administration Tools to modify the logic of the parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. This user is typically an employee of a specific Oracle Financial Services customer.
- **Oracle Financial Services Development Team:** This user is responsible for developing the Oracle Financial Services scenarios and the user interface, which are based entirely on the data that the TSDs and FSDM provide.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Supervisor:** This user works in the application on a daily basis and is typically a higher level Analyst or Compliance Officer.

How this Guide is Organized

The *Fraud Detection Technical Scenario Description* includes the following topics:

- Chapter 1, *Introduction*, describes the classes that are explained in the guide.
- Chapter 2, *How to Read the Technical Scenario Descriptions*, describes the layout (a description of the headings) of each technical scenario description, explains how to read the information, and provides notes on styles.
- Chapter 3, *Check and Deposit Fraud*, describes scenarios that monitor check and deposit/withdrawal activity for patterns of activities that could be indicative of fraud, counterfeiting or kiting schemes
- Chapter 4, *Funds Transfer and Electronic Payments (ACH) Fraud*, describes scenarios that monitor electronic payments, such as, funds transfer and payments completed through clearing house (ACH) mechanisms, for patterns or anomalies that could be indicative of fraudulent activity.
- Chapter 5, *Identity Theft and Account Takeover*, describes scenarios that monitor for activities or patterns that could be indicative of identity theft or account takeover schemes.
- Chapter 6, *ATM and Bank Card Fraud*, describes scenarios that monitor for ATM and Bank Card activity that could be indicative of fraud.
- Chapter 7, *Employee and Insider Fraud*, describes scenarios that monitor employee transactions to identify situations in which employees, acting as insiders, take advantage of access to proprietary customer and account information to defraud the institution's customers.

Technical Scenario Description - Trading Compliance

This chapter provides a high-level description of the *Oracle Financial Services Trading Compliance (TC) Solution Technical Scenario Description (TSD)*.

This chapter covers the following topics:

- About this Guide
- Who Should Use this Guide
- How this Guide is Organized

About this Guide

The Oracle Financial Services Trading Compliance (TC) Solution uses pattern recognition or scenario techniques to identify behaviors of interest, which are indicative of potentially problematic behavior. This guide outlines the scenarios included in the TC solution.

The TC scenario library provides mechanisms to help the Oracle Financial Services client monitor its internal activities, as well as its interactions with customers and other market participants. TC is able to analyze all of your trading events in the context of prevailing market conditions.

The major scenario coverage areas are organized as follows:

- **Scenario Areas:** A logical presentation of scenarios in the scenario description document.
- **Scenario Group:** A set of one or more scenarios that pertain to the same behavior of interest. Each scenario within a scenario group contains different business logic that is further refined through its specific patterns and tunable parameters.
- **Scenario:** A behavior of interest. Each scenario pertains to one focus type, an underlying pattern, and to tunable thresholds.

Who Should Use this Guide

The *Trading Compliance Technical Scenario Description Guide* is designed for use by all users of the product. Their roles and responsibilities include the following:

- **Analyst:** This user works in the application frequently. This user's specific role (Analyst I, Analyst II, or Analyst III) determines what users can see and do within the application.
- **Auditor:** This user has broad viewing rights within the application, but can perform a limited set of actions based upon the user's role as an Internal Auditor or External Auditor.
- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services Behavior Detection Platform generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.
- **Data Miner:** This user accesses the Administration Tools to modify the threshold values used by patterns to detect matches in a firm's data.
- **Executive:** This user may not be involved in the day-to-day analysis of alerts. This user can view many areas within the application but can perform only a limited set of actions.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, developing any processes needed to extract that data in the form that Oracle Financial Services requires, and delivering that data to Oracle Financial Services.
- **Oracle Financial Services Administrator:** This user accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. This user is typically an employee of a specific Oracle Financial Services customer.
- **Oracle Financial Services Development Team:** This user is responsible for developing the Oracle Financial Services scenarios and the user interface, which are based entirely on the data that the TSDs and FSDM provide.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Supervisor:** This user works in the application on a daily basis and is typically a higher level Analyst or Compliance Officer with confidential information held by the Firm on a security.

How this Guide is Organized

The *Trading Compliance Solution Technical Scenario Description* includes the following topics:

- Chapter 1, *Introduction*, describes the classes that are explained in the guide.
- Chapter 2, *How to Read the Technical Scenario Descriptions*, describes the layout (a description of the headings) of each technical scenario description, explains how to read the information, and provides notes on styles.
- Chapter 3, *Best Execution—Equities*, examines prices and timing of orders and executions by comparing them to market conditions. The scenarios generate alerts when customers did not get the best execution of their orders.
- Chapter 4, *Trading Compliance—Equities*, describes scenarios used to monitor trading activity of the Equity asset class, covering specific rules and regulations and other global trading behaviors of equity securities that are traded either on-exchange or OTC.
- Chapter 5, *Trading Compliance—Control Room*, describes detecting trading behaviors that violate the Chinese Wall policies and procedures established by the Firm or on those with confidential information held by the Firm on a security.
- Chapter 6, *Scenario Wizard Templates*, provides templates for developing scenarios which detect specific behaviors of interest via the Scenario Wizard tool.
- Appendix A, *Scope of Trading Compliance*, provides a mapping of scenarios to specific parameters and their associated data streams.

This appendix provides a brief overview of the purpose, scope, and organization of the documentation library within the Know Your Customer (KYC) Application set in the section About KYC.

About KYC

Know Your Customer (KYC) is used by financial institutions, which are required to perform appropriate risk-based due diligence when a customer opens an account. KYC also allows financial institutions to understand their customers throughout the relationship. Properly assessing the customer risk during the account opening process as well as during the life of the relationship is critical to financial institutions.

The KYC product provides the following documents:

- *KYC Risk Assessment Guide*
- *KYC Service Guide*
- *KYC Administration Guide*
- *KYC Data Model Reference Guide*

KYC Service Guide

The *Service Guide* for Oracle Financial Services® Know Your Customer (KYC) is used for specifying the exact source business data format provided to the KYC application. This guide also explains the data interface specification for the Real Time Account On-Boarding Risk Assessment service request from an external account, at the time of the account opening.

This guide is designed for use by the technical staff, database programmers and system administrators of the Oracle client.

KYC Risk Assessment Guide

The *KYC Risk Assessment Guide* provides information related to risk assessments being performed on a customer to adhere to the norms of Know Your Customer (KYC). It also covers different risk models with the parameters considered for assessing the risk a customer poses to a financial institution.

This guide is designed for a variety of Oracle Financial Services KYC users. Their roles and responsibilities, as they operate within the Oracle Financial Services KYC application, include the following:

- **Business Analyst:** A user in this role analyses and disposes the risk assessments promoted to a case. This user should understand how risk assessments are calculated and promoted to a case. A Business Analyst guides the Administrator to fine tune the parameters required for risk assessments.
- **Relationship Manager:** A user in this role verifies the risk assessments which are on hold status. This user is responsible for confirming customer information.
- **KYC Administrator:** This user is a manager for data center activities and application administration activities in a financial institution. This user has access to configuration functionalities, and is responsible for

configuring the required details for KYC process to execute. This user should have in-depth knowledge of all modules of KYC to perform the necessary administration and maintenance.

KYC Administration Guide

The *KYC Administration Guide* provides comprehensive instructions for proper system administration, and the daily operations and maintenance of OFS KYC. The logical architecture provides details of the KYC process for a better understanding of the pre-configured application, which allows you to make site-specific enhancements using OFSAAI.

The *KYC Administration Guide* is designed for use by Installers and System Administrators. Their roles and responsibilities, as they operate within the KYC, include the following:

- **Oracle KYC Installer:** Installs and configures the KYC at a specific deployment site. The Oracle Installer also installs and upgrades any additional Oracle solution sets and requires access to deployment-specific configuration information (for example, machine names and port numbers).
- **System Administrator:** Configures, maintains, and adjusts the system, and is usually an employee of a specific Oracle customer. The System Administrator maintains user accounts and roles, monitors data ingestion and alert management, archives data, loads data feeds, and performs post-processing tasks. In addition, the System Administrator can reload cache. However, the scenario description is not visible to the System Administrator.

KYC Data Model Reference Guide

The *KYC Data Model Reference Guide* provides comprehensive instructions for users responsible for customer risk analysis.

The *KYC Data Model Reference Guide* is designed for use by Oracle Financial Services client Business Analysts and Information Technology (IT) Support Staff, as well as for use by the Oracle Financial Services Professional Services and Development Teams. Their roles and responsibilities include the following:

- **Business Analyst:** This user analyzes the nature of the alerts that the Oracle Financial Services KYC generates. The Business Analyst needs a semantic understanding of the data provided in the FSDM to manage their alerts successfully. This user also provides guidance to the IT Support Staff regarding what client data to source for KYC.
- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that KYC requires, developing any processes needed to extract that data in the form KYC requires, and delivering that data to KYC.
- **Oracle Financial Services Professional Services Team and Partners:** This user is responsible for the deployment of KYC at the client's installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to KYC.
- **Oracle Financial Services Development Team:** This user is responsible for developing the KYC user interface, which is based entirely on the data that the FSDM provides.

This appendix provides a brief overview of the purpose, scope, and organization of the documentation library within the Currency Transaction Reporting (CTR) Application set in the section About CTR.

About CTR

As part of Regulations and Compliances, organizations are required to perform appropriate analysis and report any suspicious activities which may lead to fraud or money laundering within the institution to the regulatory authorities. These regulatory bodies are responsible for safeguarding financial institutions and consumers from abuse, providing transparency in the country's financial system, enhancing that country's security, and deterring and detecting criminal activity in the financial system.

Currency Transaction Reporting (CTR), which currently applies only for Currency Transaction Reports in the United States, is a robust solution developed to meet operational and regulatory requirements of the Financial Crimes Enforcement Network (FinCEN). This product helps minimize repetitive data entry and supports parallel processing of Currency Transaction Reports. CTR also helps in reducing the process cycle time using STP (Straight Through Processing) and accommodates FinCEN compliance and real time environmental changes. This product automates the workflow, analysis and report production and offers integration capabilities with internal and external systems thereby improving the operational efficiency.

CTR supports the e-filing of cash transactions that are greater than \$10,000 or multiple transactions that aggregate to greater than \$10,000. The Currency Transaction Reports are created either at the branches or through the end of day files, where CTR aggregates multiple transactions performed at the branch, ATMs and Vaults. In addition, this application also captures and reports Monetary Instrument Purchases.

A Currency Transaction Report can be created in the following ways:

- *System Generated Currency Transaction Reports*
- *Manual Creation of Currency Transaction Reports*
- *Branch Generated Currency Transaction Report*

The CTR product provides the following documents:

- *CTR User Guide*
- *CTR Administration and Configuration Guide*

CTR User Guide

The *CTR User Guide* for Oracle Financial Services® Currency Transaction Reporting (CTR) explains the concepts of the Oracle Financial Services Currency Transaction Reporting and provides step-by-step instructions for navigating the Currency Transaction Reporting (Currency Transaction Report) user interface such as viewing, verifying, reviewing, approving, e-filing of the Currency Transaction Reports with FinCEN, creating Exemptions, and managing the Currency Transaction Report process flow.

This guide is designed for use by a variety of Oracle Financial Services users. Their roles and responsibilities, as they operate within the CTR, include the following:

- **Analyst:** This user is typically responsible for updating the status of listed Currency Transaction Reports through UI screens.
- **QA Analyst:** This user is responsible for verifying the details in the Currency Transaction Reports when the status of Currency Transaction Report is changed to Pending QA review. This user role will have access to Batch Approval action of Currency Transaction Reports.
- **Supervisor:** This user is typically responsible for verifying, reviewing and approving the Currency Transaction Reports before they are e-filed with the FinCEN. This user is also responsible for managing the workflow of Exemptions.
- **E-File Analyst:** This user is responsible for e-filing the Currency Transaction Reports with the regulatory authorities once verified by the QA Analyst. This user is responsible for changing the status of Currency Transaction Reports from Ready for E-File to Filed.
- **Exemption Analyst:** This user is responsible for creating and managing the Exemptions through the UI screens.
- **Administrator:** This user is responsible for managing the static data used in the application, creating application users, mapping users to user roles, and configuring the various parameters used in the CTR.

CTR Administration and Configuration Guide

The *CTR Administration and Configuration Guide* explains the concepts behind the Oracle Financial Services Currency Transaction Reporting, and provides comprehensive instructions for proper system administration, as well as daily operations and maintenance.

Disclaimer: In this guide, Oracle Financial Services Currency Transaction Reporting and Oracle Financial Services Behavior Detection Platform are used interchangeably. As an Administrator, you can configure and manage both Oracle Financial Services Currency Transaction Reporting and Oracle Financial Services Behavior Detection Platform systems.

This guide is designed for use by Financial Services Installers and System Administrators. Their roles and responsibilities, as they operate within Oracle Financial Services Currency Transaction Reporting and Oracle Financial Services Behavior Detection, include the following:

- **Financial Services Installer:** This user installs and configures the Oracle Financial Services Applications and the client-specific solution sets at a deployment site. This user also installs upgrades, and additional solution sets. It requires access to deployment-specific configuration information (For example, machine names, and port numbers).
- **System Administrator:** This user configures, maintains, and adjusts the system and is usually an employee of a specific Oracle client. The System Administrator maintains user accounts and roles, archives data, and loads data feeds.

This appendix provides a brief overview of the purpose, scope, and organization of the documentation library within the Foreign Account Tax Compliance Act Management (FATCA Management) Application set in the section About FATCA Management.

About FATCA Management

The Foreign Account Tax Compliance Act (FATCA) is a regulation from the Internal Revenue Service and the US Treasury Department to prevent US Taxpayers who hold financial assets in non-US financial institutions (foreign financial institution or FFIs) and other offshore vehicles from avoiding their US tax obligations. US taxpayers' investments have become increasingly global in scope. FFIs now provide a significant portion of the investment opportunities for, and act as intermediaries with respect to the investments of, US taxpayers. Like US financial institutions, FFIs are generally in the best position to identify and report with respect to their US customers and substantial US owners. The intent behind the law is for FFIs to identify and report US citizens who may have accounts or investments with the FFI.

In order to comply, FFIs are required to enter into an agreement with the US Treasury or comply with intergovernmental agreements (IGAs) entered into by their local jurisdictions. Failure to enter into an agreement or provide required documentation will result in the imposition of a withholding tax (currently specified as 30%) on certain payments (US source Fixed, Determinable, Annual, Periodical (FDAP) income) made to such customers or counterparties. Failure to impose the requisite withholding under FATCA requirements could result in significant financial exposure.

For details regarding the FATCA regulations, refer to the IRS or US Treasury links:

<http://www.irs.gov/Businesses/Corporations/Foreign-Account-Tax-Compliance-Act-FATCA>

The FATCA Management product provides the following documents:

- *FATCA Assessment Guide*
- *FATCA Management Administration and Configuration Guide*
- *FATCA Data Model Reference Guide*

FATCA Management Assessment Guide

The *FATCA Management Assessment Guide* provides information related to Foreign Account Tax Compliance Act (FATCA) assessments being performed on an Account or Customer to adhere to the norms of FATCA regulation from the United States Internal Revenue Service (IRS). It also covers the parameters considered for creating cases on those assessments. Cases allow institutions to do further due diligence and manually update the FATCA status of an Account or Customer.

This guide is designed for a variety of OFSFATCA Management users. Their roles and responsibilities, as they operate within the OFSFATCA application, include the following:

- **FATCA Analyst:** This user analyzes and disposes the assessments which have been promoted to a case. This user should understand how assessments are done, FATCA statuses are assigned and assessments are manually promoted to a case. A FATCA Analyst guides the Administrator to fine tune the parameters required for assessments.

- **FATCA Supervisor:** This user monitors and verifies actions taken on FATCA cases. This user is responsible for any update to the FATCA status in Enterprise Case Management.
- **FATCA Administrator:** This user is a manager for data center activities and application administration activities in a financial institution. This user has access to configuration functionalities, and is responsible for configuring the required details for FATCA processes to execute. This user should have in-depth knowledge of all parameters and rules used in FATCA Assessment. In addition, this user is informed on the necessary administration and maintenance functionalities.
- **FATCA Auditor:** This user monitors the FATCA assessments and cases. This user has read only access on FATCA assessments and cases.

FATCA Management Administration and Configuration Guide

The *FATCA Administration and Configuration Guide* explains the structure behind the Oracle Financial Services Foreign Account Tax Compliance Act (OFS FATCA) and provides comprehensive instructions for configuring modifiable components. It provides comprehensive instructions for proper system administration, as well as daily operations and maintenance.

This guide is designed for Oracle Financial Services Installers and System Administrators. Their roles and responsibilities, as they operate within Oracle Financial Services FATCA, include the following:

- **FATCA Administrator:** Configures, maintains, and adjusts the system and is usually an employee of a specific Oracle Financial Services customer. The System Administrator maintains user accounts and roles, monitors data ingestion and case management, archives data, loads data feeds, and performs post-processing tasks.
Note: A FATCA Administrator must also be assigned with the Mantas AM Administration Group for mapping the FATCA cases to owners. For more information on mapping the User(s) to User Group(s) and mapping the User Group(s) to Domain(s), refer to section *Mapping User Group(s) to Domain(s)* in *Administration Guide*.

FATCA Management Data Model Reference Guide

The *FATCA Management Data Model Reference Guide* provides comprehensive instructions for the generation of FATCA Management and FATCA Regulatory Reporting.

Through the use of AAI's Rules Framework, Oracle executes a series of rules that are designed to assess accounts and customers on a variety of criteria to determine their status as US persons and if they qualify for reporting to the IRS and / or require withholding of funds to satisfy the US tax laws. If your firm has implemented Oracle Financial Services FATCA Management, the tables within this guide describe how the FSDM captures both configuration and results information related to execution of the FATCA rules. If your firm has implemented Oracle Financial Services FATCA Regulatory Reporting these tables capture both configuration and results information related to the filing of FATCA regulatory reports.

This guide is designed for use by various users of Oracle Financial Services applications. Their roles and responsibilities, as they operate within FATCA Management, include the following:

- **Business Analyst:** This user should have an in-depth understanding of the data provided to FATCA RR in order to manage the report requests successfully. The Business analyst should also provide guidance to the IT Support Staff regarding what client data to source for Oracle Financial Services.

- **IT Support Staff:** This user is responsible for identifying the appropriate client data sources that Oracle Financial Services requires, and for developing any processes needed to extract that data in the form required by Oracle Financial Services, as well as delivering that data to Oracle Financial Services.
- **Oracle Financial Services Professional Services Team:** This user is responsible for the deployment of Oracle Financial Services at the clients' installation site. The Oracle Financial Services Professional Services Team provides guidance and assistance in the identification and delivery of data to Oracle Financial Services.
- **Oracle Financial Services Development Team:** This user is responsible for developing Oracle Financial Services scenarios and the User Interface (UI), which are based entirely on the data that FATCA Management provides.

