ORACLE
Financial Services

Oracle Financial Services Customer Screening

Technology Guide

ORACLE BEST PRACTICE GUIDE | JUNE 2018

Table of Contents

1.0 Document Purpose

This document provides an overview of the capabilities and technical components of Oracle Financial Services Customer Screening, a risk and compliance screening application.

This document is intended to give IT staff an understanding of how Oracle Financial Services Customer Screening functions, what the key inputs to screening are an how to manage these and what technical components are required.

2.0 Oracle Financial Services Customer Screening Overview

The primary function of Oracle Financial Services Customer Screening is to provide an end-to-end process for matching any individual or entity against entries on various watchlists.

There are many watchlists against which an organization may, for regulatory or risk purposes, be required to screen individuals and entities when initiating a business relationship. These include sanctions lists published by governments or economic, political, and law enforcement bodies. Lists published by commercial sources, such as politically exposed person (PEP) lists, and internal blacklists created by companies themselves may also be required for review.

Sanctions lists contain entries of debarred individuals or entities due to involvement in criminal activity such as money laundering, international terrorism, and financial crime. Sanctions lists may also include lists of embargoed countries.

PEP lists contain entries of high-profile (and often high-value) public figures, such as business leaders, prominent social figures, and members of political parties. Due to their position in society, their political position, or associations and relationships with other high-profile parties, PEPs may be subject to potential bribery or misuse their power and influence for personal gain or financial advantage.

For simplicity, all such watchlists are referred to as reference data throughout the remainder of this document.

2.1 High-Level Overview

Oracle Financial Services Customer Screening runs on the Oracle Enterprise Data Quality platform, for data optimization and matching, and Oracle Financial Services' Analytical Applications Infrastructure, Financial Crime Data Model and Enterprise Case Management, and therefore shares common hardware with other Financial Crime and Compliance Management products. Built upon a modular architecture, it can be tailored to meet the compliance screening processes specific to each industry; the types of records being screened; the match rules applied; and the processes for investigating, managing, and escalating any potential match. Hence Oracle Financial Services Customer Screening includes configurable data optimization, matching, and case management modules to provide tailored solutions to meet the specific needs of each customer.

Data optimization prepares both customer and watchlist data ahead of matching to ensure that any errors and variances in both the structure and content of data are resolved. Matching takes the output from the data optimization module and attempts to determine potential matches between records contained in list data sources and customer data. Those records that exhibit a close match are then presented to case management for investigation and resolution by the compliance team.

An overview of Oracle Financial Services Customer Screening and its functional components is shown in Figure 1.

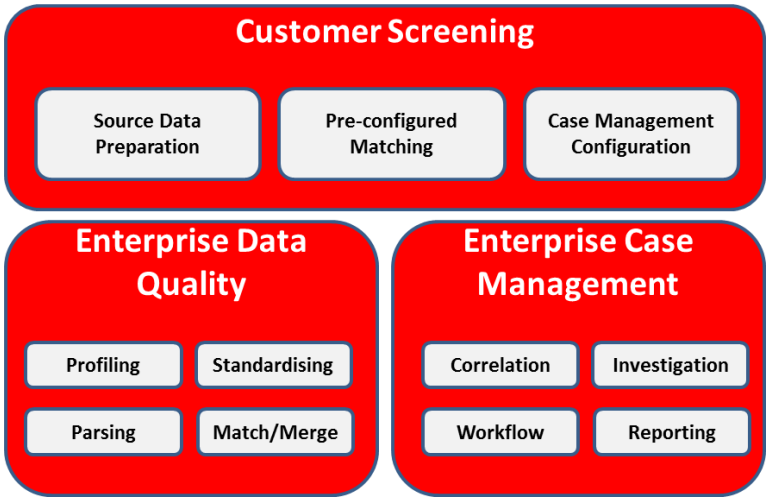

Figure 1. An overview of Oracle Financial Services Customer Screening and its functional components.

Oracle Financial Services Customer Screening can screen records in both batch and real time, making it suitable for a range of use cases including client on-boarding and regular screening of existing customers.

2.2 Oracle Financial Services Customer Screening Architecture

Oracle Financial Services Customer Screening has an advanced matching and screening engine, containing a suite of configurable match rules for determining both exact and fuzzy matches between working (customer data) and reference data. Customer Data is first loaded into the Financial Crime Data Model via a common staging area, and is then standardized prior to matching. Watchlist data from multiple external providers and customer internal lists is also standardized for maximum matching efficiency. Screening is run to compare all customer records against all watchlist records to create new matches where records of either type have been added or changed. Matching results are compared to previous results to ensure only new and changed events are promoted to case management. Event data is correlated and cases which require review are created within Enterprise Case Management. Figure 2 shows each component of Oracle Financial Services Customer Screening in more detail and illustrates how each of these interacts in a standard implementation.

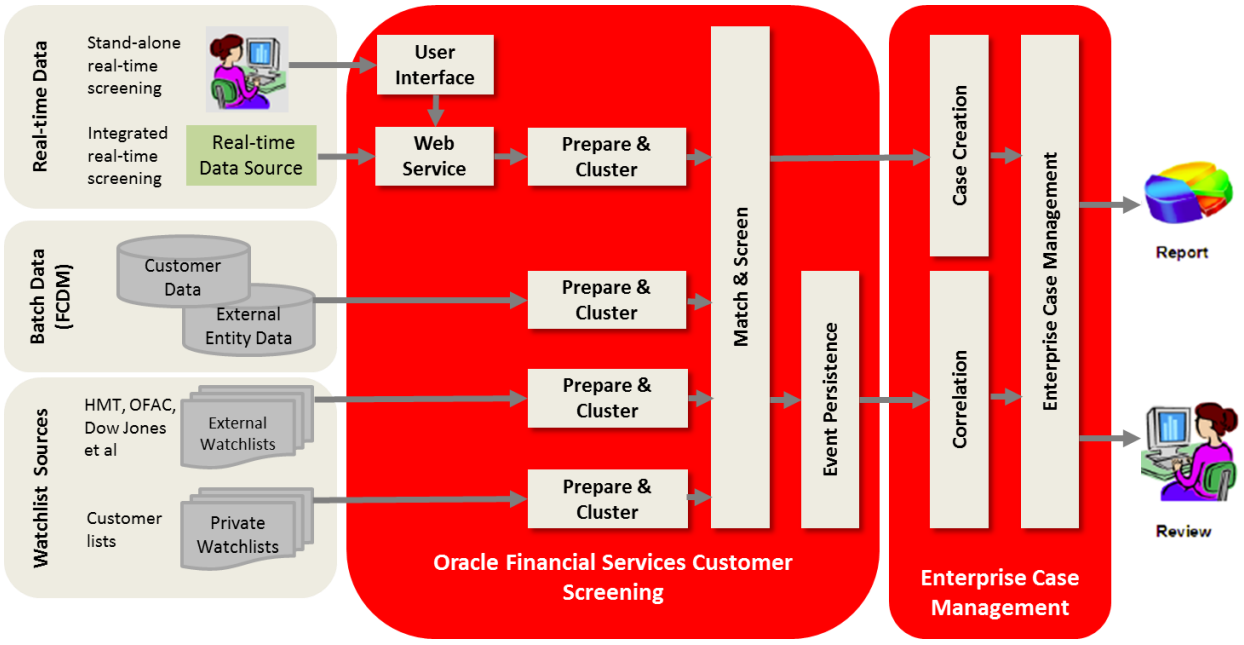

Figure 2. How each component of Oracle Financial Customer Screening interacts in a standard implementation.

2.2.1 Connecting to Data Sources

Oracle Financial Services Customer Screening uses database connectors to connect to both Financial Crime Data Model (customer) data and to each of the external reference data sources, as shown on the left in Figure 2.

Working data may persist in a number of databases and repositories across the organization, often using various file formats. Oracle Financial Services Customer Screening can work with any type of customer data, the preparation of which is normally part of system configuration at the time of implementation. Where required Oracle Enterprise Data Quality can be used to standardize and improve data prior to loading into the Financial Services Crime Model. Oracle Enterprise Data Quality provides transliteration and transcription support for global deployments.

Providers of reference data sources publish their list data in various files and formats, and Oracle Financial Services Customer Screening includes a preconfigured connector to each of the most common sources. See section 4 for more details.

2.2.2 Preparation and Clustering

Data preparation is a crucial element of the process and has a direct impact on the accuracy of the screening process, the elimination of risk, and the reduction of false positives for the compliance team to review.

For reference data sources, preparation and clustering are carried out as the same process because the list data is presented in a known format. For customer data, preparation and clustering are normally undertaken separately, because the often unstructured nature of this data requires the use of comprehensive on-board utilities to prepare the data ahead of the clustering process.

2.2.3 Matching and Screening

The matching and screening component of Oracle Financial Services Customer Screening provides sophisticated fuzzy logic, combined with advanced data optimization techniques to ensure highly accurate screening. Effective screening relies upon non-exact complex fuzzy matching, because criminal elements targeting organizations often transpose names, dates of birth, and other personal information in an attempt to conceal their true identity.

Oracle Financial Services Customer Screening also uses secondary identifiers as part of the screening process. This allows the software to differentiate between individuals and entities with common names along with a large number of discrete match rules available that can be activated. With the correct application of these to customer and list data sources, false positives can be reduced to a minimum without increasing risk.

2.2.4 Event Persistence

All customer screening matches are held in the Financial Crime Data Model. The persistence functionality promotes only items which require review into Oracle Financial Services Enterprise Case Management, while providing confidence all records are being checked for changes in customer or watchlist data.

2.2.5 Correlation

Correlation allows clients to apply logic to group similar events into a case, thus enabling individuals to spend less time sifting through a large number of individual cases. By default, Oracle Financial Services Customer Screening will bring together all potential Sanctions events for a customer to aid decision making. Politically Exposed Person and Enhanced Due Diligence events will be grouped separately to allow different prioritization, assignment and process. The correlation functionality is configurable to provide flexibility and efficiency around specific business process and organizational models.

2.2.6 Case Management

Customer Screening cases contain multiple Events. One Event is created for each Watchlist record which generates matches for the customer record. Events may have multiple matches associated with them if there are alias records for the same Watchlist Id. Within a case, false or true positive decisions will be made against each Event. Each case is allocated to a workflow, enabling the investigation to progress in a structured way. Cases are given a priority using a match strength score (or in some cases, combined match and risk score) and assigned to case reviewers for investigation.

Case management also provides comprehensive audit tools that enable attachments to be appended to capture a full history of all decisions and state changes applied.

There are 3 different case types for Customer Screening for Sanctions, Politically Exposed Persons and Enhanced Due Diligence and 2 default workflows, one for Sanctions and the other which is used by both Politically Exposed Persons and Enhanced Due Diligence Cases. These can be amended for specific customer requirements via Case Designer and Process Modelling Framework if required.

2.2.7 Configuration Reporting

Configuration management features provided by Oracle Enterprise Data Quality make it easy to manage, audit, and share match rules across the organization, ensuring that all business units are fully optimizing their screening processes. The configuration management features enable the user to:

- Create “configuration diffs” on an ad hoc basis
- Save the results in a format that can be read using common tools
- More easily diagnose problems in a particular implementation

Screening configurations can be published as reports, making it easy to conduct an audit of match rules applied across a broad spectrum of risk profiles. This provides an extra layer of auditing by making it simple to determine whether and how match rule configurations have changed compared with the configuration at a previous point in time. This is particularly important for demonstrating robust procedures and effective due diligence during any investigation undertaken by the regulator.

2.2.8 Management Reporting

Oracle Financial Services Customer Screening can be integrated with Oracle Financial Services Crime and Compliance Management Analytics for business intelligence and analytical reporting.

3.0 Screening Schedules and Data Flows

The screening process should be run on a regular basis in order to detect new potential matches. The frequency of runs will be defined by the compliance team and will be based on their view of risk. The majority of Oracle's customers screen every 24 hours.

Due to the nature of data changing in both the working and reference datasets, it is imperative to screen all customer data against all of the reference data lists, and not just the new and changed records. This is made possible using the powerful matching engine in the Oracle Enterprise Data Quality platform, which is able to process very large datasets on modest hardware. Intelligent algorithms for suppressing repetitive possible matches (often called false positives) reduce the workload on the review user.

Data to be screened can be derived from either real-time sources (for example, via Oracle Financial Service Know You Customer or integrated with another Front Office application) or in batch mode during regular screening cycles of existing customers or external entities.

Both screening methods can be run concurrently, enabling screening during on-boarding of new customers to be undertaken at the same time that regular checks are being carried out on existing individuals and entities.

3.1 Preparing Data for Screening

Oracle Financial Services Customer Screening employs advanced data-preparation techniques to ensure that customer and list data is optimized to match rules. This is necessary to achieve a high degree of accuracy in the screening process, minimizing high numbers of false positives and the potential for false negatives. Processes to interpret the data, understand it, and optimize it for screening are provided by Oracle Financial Services Customer Screening, including parsing out multiple names in a single field, finding names in address fields, and spotting multiple names in name fields. These are all potential data quality issues.

3.2 Working with International Data

Oracle Financial Services Customer Screening provides optional language packs to enable customers to screen data held in non-Latin script. Language packs provide language-specific rules to enable screening of data in non-Latin format against lists that hold names in Latin form. This normally involves a transliteration processor, with associated reference data, and a dictionary of name variants. The transliteration processor is used in customer data preparation, and the reference data in matching.

Language packs are offered as:

- Basic (transliteration only)
- Medium (transliteration and name variant dictionary)
- Complex (third party data and extensions to handle transcription)

The type of language pack required depends upon the writing system used to capture the original customer record. For example, a basic language pack will be required for screening customer data held in the Greek alphabet, whereas Arabic would require the complex language pack.

3.3 Match and Risk Scoring

Match Scoring is a function of how close a match exists between an individual or entity and an entry on one or more watchlists—the closer the match, the higher the score. The event match score will be the maximum of all scores for matches within that event. This capability is delivered out-of-the-box as part of Oracle Financial Services Customer Screening.

Oracle Financial Services Customer Screening also offers the option of a risk scoring module to complement its match score capabilities. Risk scoring enables a further layer of data preparation to take place ahead of screening, making it easier to prioritize potential matches in line with the organization's risk tolerance.

Risk scoring works by allocating a value to one or more attributes in both customer data and watchlist entries that may be seen as factors contributing to risk, such as country of residence, occupation, membership of a particular regime, product holdings, and investments.

Should a match be found against any individual or entity, the combined value of the match score and the risk score will be included within the Event presented to case management, and the entry will be prioritized accordingly. This makes it easier to prioritize review activity against those Events that present the greatest potential threat to the organization.

3.4 Batch Screening

Batch screening of working data against reference data sources usually takes place at periodic intervals (for example, on a daily basis, often overnight), with results being made available for compliance teams at the start of the next working day. Both working and reference data are downloaded into a set of repositories via a suite of standard out-of-the-box connectors and are prepared in readiness for matching. The process workflow for batch screening can be summarized as follows:

- The chosen sanctions/PEP lists, referred to as reference data, are read into the Oracle Enterprise Data Quality server for matching.
- Customer data loading from Staging Tables into the Financial Crime Data Model and is then read into the Oracle Enterprise Data Quality server and prepared for matching.
- The matching process is then run to identify exact and potential matches between working and reference data.
- Match data is written to Financial Crime Data Model and checked against persisted data.
- New and changed Event data is correlated to generate or update Cases in Enterprise Case Management.
- Matching can be run at the same time as investigators are working on the cases.

The compliance team accesses and reviews the results of the matching process in Oracle Financial Services Enterprise Case Management.

3.5 Real-Time Screening

The capability to screen walk-in clients in real time is offered via the Customer Screening Application or as an application-independent REST API. This gives customers the option of choosing either Oracle Financial Service Know Your Customer, or using their own real-time screening client interface and integrating this with Oracle's comprehensive screening engine.

3.5.1 Customer Integrations

Oracle Financial Services Customer Screening exposes a REST API to support customers who wish to use their own bespoke UI for real-time screening. This enables screening processes to be tailored to suit business practice, such as how to process records when a potential match is found, and the level of information disclosed to the user.

- Oracle Financial Services Customer Screening can easily be integrated and used within an existing front-office application, new dedicated application or portal Web page and is accessed.

» In real-time mode, Process Modelling Framework orchestrates the screening of the record in Enterprise Data Quality, the generation of cases and events in Enterprise Case Management and the returning of case summary details.

3.5.2 Real-Time Screening in Action

Figure 3 illustrates a real-time screening workflow where an organization chooses to integrate Oracle Financial Services Customer Screening with its own customer on-boarding system.

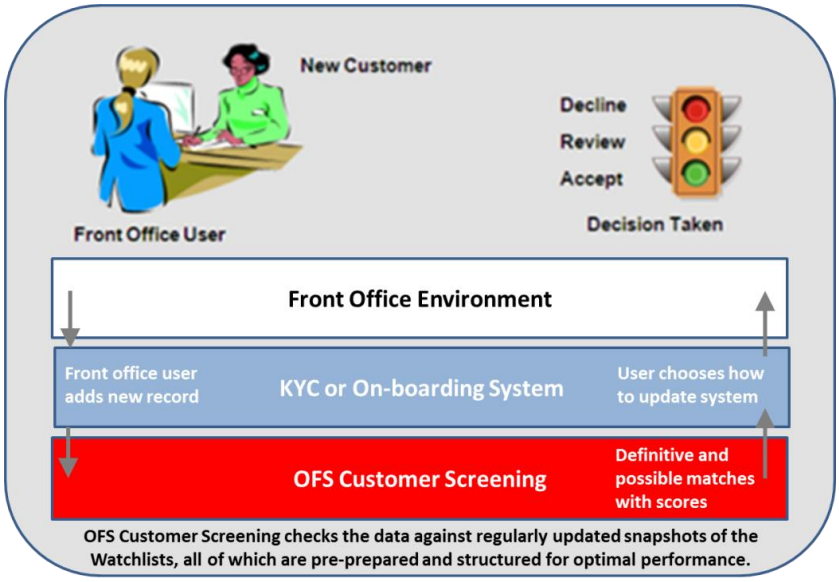

Figure 3. Oracle Financial Services Customer Screening is integrated with a custom on-boarding system.

3.6 Ad Hoc Screening

Ad hoc screening is often carried out at the end of each day, when lists of individuals and entities are submitted to a central team of compliance workers for screening. These records are then uploaded for screening as a batch file. Real-time screening refers to the screening of walk-in customers at the time they make a request for service, such as for parcel shipment or account opening. For all intents and purposes, ad hoc screening follows the same process as for batch screening, and is possibly best thought of as batch screening on demand.

4.0 Working Data

4.1 Customer Data

Oracle Financial Services Customer Screening uses Customer and Customer Address data from the Financial Crime Data Model for screening. Cases also have account information to aid investigation.

Customer data from screening is standardized for the purposes of screening prior to matching.

During this transformation process, data quality issues—such as superfluous data after surnames—are assessed and rectified. The Oracle software will not change the source data during its processing; all changes occur internally to Oracle Enterprise Data Quality. The data used for matching within Oracle Financial Services Customer Screening is categorized as either an entity or an individual, defined as follows.

4.2 Entities

This category covers entities including organizations, companies, charities, and political parties.

Table 1 shows the attributes that are mandatory (M) and optional (O) when screening records of entities against watchlist sources. Where risk scoring is deployed, additional data attributes (X) can be used in the matching process to assist in prioritizing review work in line with criteria defined by the compliance team. Underlying directors or beneficial owners are treated as individuals for the purpose of screening.

TABLE 1. CERTAIN CRITERIA ARE MANDATORY (M) AND OTHERS OPTIONAL (O) WHEN SCREENING ENTITIES FOR RISK.

Data Field	Type	Risk Scoring
Customer Identifier	M	
Organization Name	M	
Alias Name	O	
Country of Incorporation	O	X
Country of Operation(s)	O	X
Address City	O	
Address Country	O	X
Company Registration Number	O	
Industry Code/Type	O	X
Products	O	X

4.3 Individuals

Similar to the screening for entities illustrated in Table 1 above, Table 2 shows the attributes that are mandatory (M) and optional (O) when screening records of individuals against watchlist sources:

TABLE 2. CERTAIN CRITERIA ARE MANDATORY (M) AND OTHERS OPTIONAL (O) WHEN SCREENING INDIVIDUALS FOR RISK.

Data Field	Type	Risk Scoring
Customer Identifier	M	
Title	M	
First Name(s)	M	
Middle Name	O	
Family Name	M	
Full Name	M	
Alias	O	
Date of Birth	O	
Age	O	X
Gender	O	X
Country of Residence	O	X

Country of Birth	O	X
Address City	O	
Address Country	O	
Primary Citizenship	O	
Secondary Citizenship	O	
Product(s)	O	X
Occupation	O	X

4.4 Reference Data

Oracle Financial Services Customer Screening works with all national, regional, and global sanctions and watchlists, including but not limited to:

- Government Lists
  - Her Majesty's Treasury (HMT) sanctions list
  - US Office of Foreign Asset Control (OFAC) sanctions list
  - European Union (EU) sanctions lists
  - UN (United Nations) sanctions lists
- Commercial Watchlists including those provided by:
  - Accuity
  - Dow Jones
  - World-Check
- External Risk Score Providers
  - Safe Banking Systems (SBS)

Customers' own blacklists or other denial lists can also be included and used as reference data for screening through simple configuration changes.

For all major open source and commercial sources, Oracle has designed preconfigured connectors that are able to read in the data from the source and prepare it for matching. It is also possible (if required) to automate the collection of this watchlist data. A process is loaded within Oracle Financial Services Customer Screening to enable the connector to reach out and read the list data.

While Oracle provides the required connectors as part of Oracle Financial Services Customer Screening, it is the customer's responsibility to sign a contract with each of the commercial list providers in order to gain access to the list data. Open source lists (such as those provided by government agencies) are available as an anonymous download and require no subscription or contract.

5.0 System Architecture

Oracle Financial Services Customer Screening can be deployed as part of a larger Financial Crime and Compliance Management implementation or as a stand-alone deployment.

An Oracle Financial Services Customer Screening implementation consists of:

- Financial Crime Data Model
- Oracle Enterprise Data Quality
- Oracle Financial Services Customer Screening

» Oracle Financial Services Enterprise Case Management

The recommended architecture will depend on a number of factors such as:

» Whether Customer Screening is standalone or part of an FCCM deployment
» Whether batch and real-time screening will be run
» Volumes of customer and other data
» High availability requirements
» Disaster recovery and back-up and restore requirements

Architecture and sizing recommendations for specific implementations can be provided by Oracle Financial Services Consulting Team.

Appendix 1: Glossary of Terms

Term	Definition
Ad hoc screening	Screening that takes place outside of normal processes.
Batch screening	Periodic screening of a customer (or working data) against reference data sources.
Blacklists	Customer's records of individuals and entities denied a service.
Fuzzy matching	Matching based on reasoning that is approximate rather than accurate.
Case	A collection of related events with a distinct lifecycle. A single case may be generated where a customer record matches one or more watch-list records.
Case management	A suite of integrated tools for investigating and reporting on potential matches.
Configuration comparisons	Used to highlight the similarities and differences of configuration between two components or sets of components.
Customer data	Records of individuals and entities held by the organization.
Data optimization	The processes applied in preparing data in readiness for screening (for example, profiling, parsing, and deduplication).
Event	A potential match between a customer and watchlist entry presented ot case management for review.
False positive	A potential match that is not true but is presented as such.
False negative	A true match that was not identified.
Matching	A comparison of two or more records to determine whether or not a relationship exists.
Match score	A numeric value attributed to a particular match rule that caused two records to be related.
MI reporting	Reports presented in a style and format suitable for executive management.
Out-of-the-box	Preconfigured and ready to install.
Politically exposed person (PEP)	A current or former official of government, a major political party, or certain corporations and his/her immediate family members, as well as any close personal or professional associate of such a person.
Real time	In the context of screening, checking for potential matches between customer and reference data on request.

Reference data	Watchlist data that is used in matching and is to be screened against.
Risk score	A score calculated for each individual or entity on each watchlist, based on various attributes such as country of residence, operating country, associated regime, and so on.
Sanctions lists	Lists published by government agencies (for example, HMT and OFAC) containing records of sanctioned individuals and entities with whom organizations are prohibited from conducting business.
Secondary identifiers	For example, date of birth, name in original script, country of residence, and photographs.
Screening	The process of determining whether a potential match exists between a customer record and one or more entries contained within list data sources published by government agencies and commercial providers.
Screening client	A client application executing on the user's machine.
Watchlist	A list available from a provider containing details of any/all of the following: sanctioned individuals, entities, PEPs, and their relatives and close associates.
Walk-in customers	Customers not having a preexisting account when requesting a service or opening an account.
Working data	Customer data held by the organization that is used in matching and is to be screened.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US


blogs.oracle.com/financialservices


facebook.com/oraclefs


twitter.com/oraclefs


oracle.com/financialservices

Integrated Cloud Applications & Platform Services

Oracle Financial Services Customer Screening: Technology Guide
June 2018