# ORACLE DATA MASKING PACK

THE INDUSTRY'S HIGH PERFORMANCE MASKING SOLUTION FOR ORACLE DATABASE APPLICATIONS

*Many organizations inadvertently breach information when they routinely copy sensitive or regulated production data into non-production environments. Data in non-production environment has increasingly become the target of cyber criminals which can be lost or stolen. Hence, like data breaches in production environment, non-production environment data breaches can incur significant cost to remediate let alone irreparable harm to reputation and brand. Oracle Data Masking Pack helps organizations reduce this risk by irreversibly replacing the original sensitive data with fictitious yet realistic data so that production data can be shared safely for non-production use.*

## KEY FEATURES

- Sensitive Data Discovery and Application Integrity
- Comprehensive and Extensible Mask Library
- Secure High Performance Mask Execution
- Sophisticated Masking Techniques
- Automatic download of templates as they become available from Oracle

## KEY BENEFITS

- Rapid sharing of production data in compliance with data privacy regulations
- Consistent and automatic enforcement of data privacy policies across all enterprise data
- Increased DBA productivity by automating the discovery and masking of sensitive data

## RELATED PRODUCTS

Oracle Data Masking Pack delivers maximum benefits when use with the following Oracle Products

- Oracle Test Data Management Pack
- Oracle Real Application Testing
- Oracle Diagnostic Pack
- Oracle Tuning Pack
- Oracle Lifecycle Management Pack

## Identifying Sensitive Data

Organizations first need to define what sensitive data they have in their environment before attempting to locate and then to mask this sensitive information. The definition of sensitive data id driven by a variety of reasons, such as company confidentiality, regulatory (Sarbanes-Oxley, PCI DSS or HIPAA compliance).

Oracle Data Masking Pack provides comprehensive capabilities allowing security administrators to define data patterns, such as 15- or 16-digits for credit card numbers, 9-digit formatted US social security numbers or UK national insurance number that can be reused to automatically discover sensitive data. The search results are ranked based on probability of match and security administrators can then designate the column as sensitive for inclusion in the data masking process or not sensitive for exclusion from future ad hoc pattern searches.

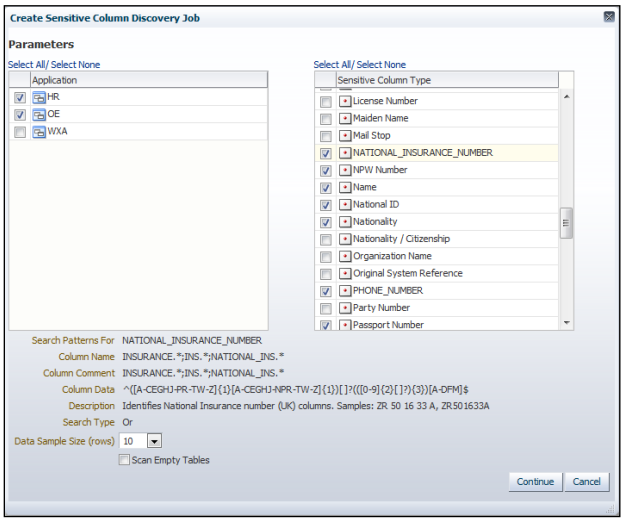



Figure 1. Sensitive data discovery

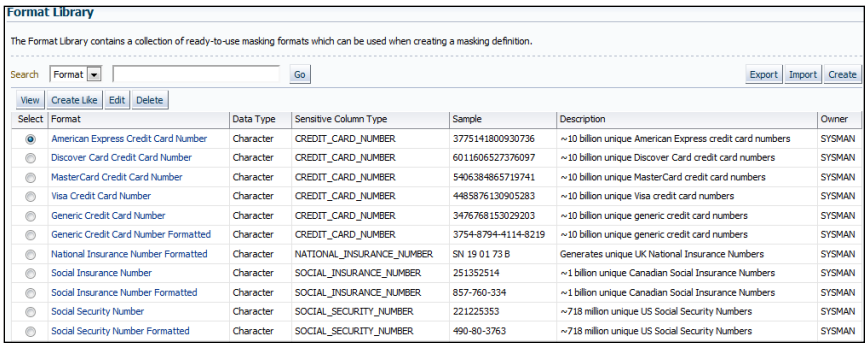
## Ensure Data Integrity

Defining and identifying sensitive data to mask is only part of the solution. With the added complexity of preserving data relationships after masking, Oracle Data Masking pack automatically detects data dependencies such as foreign key constraints ensuring referential integrity to maintain correct application behavior. For example if a secure column, employee id is a primary key in a table relationships, then all dependents will be included in the masking process so that the masked value will be consistent across the related tables enforcing referential integrity.

## Enterprise Standardized Masking

Sensitive information can come in a variety of formats and masking of sensitive information can become a very complex process to maintain correct application functionality.

To simplify, Oracle Data Masking Pack provides a centralized library of out-of-the box mask formats for common types of sensitive data, such as credit card numbers, phone numbers, national identifiers (social security number for US, national insurance number for UK). By leveraging the Format Library in Oracle Data Masking Pack, enterprises can apply data privacy rules to sensitive data across enterprise-wide databases from a single source and thus, ensure consistent compliance with regulations. Enterprises can also extend this library with their own mask formats to meet their specific data privacy and application requirements.



**Format Library**

The Format Library contains a collection of ready-to-use masking formats which can be used when creating a masking definition.

Search: Format | Go | Export | Import | Create

View | Create Like | Edit | Delete

| Select | Format | Data Type | Sensitive Column Type | Sample | Description | Owner |
|---|---|---|---|---|---|---|
| ◉ | American Express Credit Card Number | Character | CREDIT_CARD_NUMBER | 3775141800930736 | ~10 billion unique American Express credit card numbers | SYSMAN |
| ○ | Discover Card Credit Card Number | Character | CREDIT_CARD_NUMBER | 6011606527376097 | ~10 billion unique Discover Card credit card numbers | SYSMAN |
| ○ | MasterCard Credit Card Number | Character | CREDIT_CARD_NUMBER | 5406384865719741 | ~10 billion unique MasterCard credit card numbers | SYSMAN |
| ○ | Visa Credit Card Number | Character | CREDIT_CARD_NUMBER | 4485876130905283 | ~10 billion unique Visa credit card numbers | SYSMAN |
| ○ | Generic Credit Card Number | Character | CREDIT_CARD_NUMBER | 3476768153029203 | ~10 billion unique generic credit card numbers | SYSMAN |
| ○ | Generic Credit Card Number Formatted | Character | CREDIT_CARD_NUMBER | 3754-8794-4114-8219 | ~10 billion unique generic credit card numbers | SYSMAN |
| ○ | National Insurance Number Formatted | Character | NATIONAL_INSURANCE_NUMBER | SN 19 01 73 B | Generates unique UK National Insurance Numbers | SYSMAN |
| ○ | Social Insurance Number | Character | SOCIAL_INSURANCE_NUMBER | 251352514 | ~1 billion unique Canadian Social Insurance Numbers | SYSMAN |
| ○ | Social Insurance Number Formatted | Character | SOCIAL_INSURANCE_NUMBER | 857-760-334 | ~1 billion unique Canadian Social Insurance Numbers | SYSMAN |
| ○ | Social Security Number | Character | SOCIAL_SECURITY_NUMBER | 221225353 | ~718 million unique US Social Security Numbers | SYSMAN |
| ○ | Social Security Number Formatted | Character | SOCIAL_SECURITY_NUMBER | 490-80-3763 | ~718 million unique US Social Security Numbers | SYSMAN |

Figure 2. Mask Format Library

Additionally some sensitive information can reside in complex combinations which would require a sophisticated masking approach to ensure application operability. Oracle Data Masking Pack provides a variety of sophisticated masking techniques out-of-the-box to simplify the process. For example,

- **Condition-based masking:** this technique makes it possible to apply different mask formats to the same data set depending on the rows that match the conditions. For example, applying different national identifier masks based on country of origin.
- **Compound masking:** this technique ensures that a set of related columns is masked as a group to ensure that the masked data across the related columns retain the same relationship, e.g. city, state, zip values need to be consistent after masking.
- **Deterministic masking:** this technique ensures repeatable masked values after a mask run. Enterprise may use this technique to ensure that certain values, e.g. a customer number gets masked to the same value across all databases.
- **Key-based reversible masking:** when businesses need to send their data to a 3rd party for analysis, reporting or any other business process, this technique transforms the original data into a masked representation of itself using a secure key-based reversible masking function. Once the data is recovered from the 3rd party, the business can recover the original data by

reversing the masking using the same key.

## Application Data Masking Templates and Integration with Self-Update

Given the complexity of packaged applications, Oracle Data Masking Pack and data subsetting delivers meta-data knowledge of these packaged applications in the form of templates that allow you to quickly get started in masking sensitive data. The templates that are available with the latest release of Enterprise Manager are Oracle E-Business Suite and Oracle Fusion Applications.

In addition, these templates can be easily downloaded using the Self-Update feature of the latest release Oracle Enterprise Manager directly into the Software Library. Which are then immediately available to Data Masking and data subsetting. This capability also allows you to get the latest templates available from Oracle, out of band of the next major release cycle, such as the upcoming PeopleSoft template.

## At-Source Masking

Traditionally, sensitive and regulated information is obfuscated for non-production use outside of production environment. As a result this technique required system administrators to isolate and fence off the cloned environment until all sensitive data had been scrubbed and then shared. As a consequence setting up this environment took away limited key resources from productive use in addition to the added vulnerability. With the latest release of Data Masking, customers can now take advantage of masking at the source without requiring a dedicated environment. Production data can be extracted and masked and kept in masked exported files which can then be shared directly with non-production environments without affecting production data. Hence sensitive production data never leaves production environments.

## Secure, High Performance, Efficient, Integrated Mask Execution

Unlike traditional masking processes that are typically slow, Oracle Data Masking Pack uses highly efficient parallelized bulk operations to replace the original sensitive data with masked data.

Oracle Data Masking Pack also provides the ability to clone-and-mask via a single workflow. The secure high performance nature data masking combined with the end-to-end database cloning workflow ensures that enterprise can provision test systems from production rapidly instead of days or weeks that it would with separate manual processes.

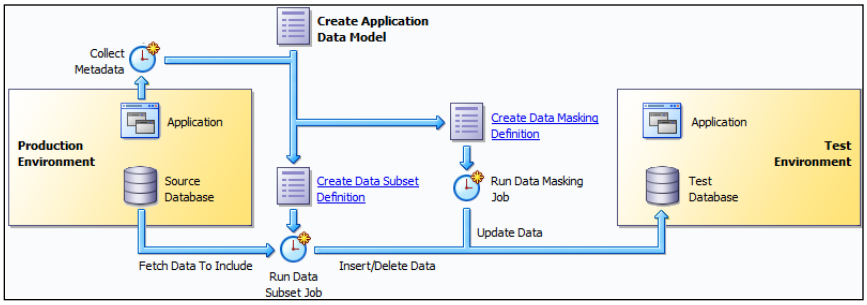



Figure 3. Integrated test data management solution

## Integrated Data Masking and data subsetting

With rapidly growing data volumes and the frequency of refreshing non-production environments such as QA, test or development, implementing an efficient, highly performing data security solution becomes a paramount challenge.

In the latest release of Data Masking Pack, to address this challenge, we have integrated the capabilities of data subsetting and Data Masking. This allows enterprises to provision a secure

and reduced size test system directly from production database without the need for a full production database copy. Enterprise may choose to execute the masking or subsetting operations or both to provision a non-production database in a single workflow from production without affecting production data.

This eliminates the need for a full copy of the production database which could incur significant storage costs and ensures that the sensitive data never leaves production.

### Secure Testing in a Masked Environment

Capturing workload from production and replaying it in a test environment to assess impact of change has proven to be the most realistic and effective type of testing. Providing this type of testing while ensuring security raises another challenge for enterprises.

The integration of Real Application Testing and Oracle Database Masking, allows data used for testing to be shared in a manner that adheres to data privacy and compliance regulations. This enhancement permits Oracle Data Masking to consistently mask across all test data artifacts with respect to application data and Real Application Testing artifacts providing the same high quality of testing in a secured environment.

### Heterogeneous Data Masking

Oracle Data Masking Pack can support masking of data in heterogeneous database, such as IBM DB2 and Microsoft SQL Server, through the use of Oracle Database Gateways

### Oracle Enterprise Manager

Oracle Data Masking Pack is one of the key capabilities integrated seamlessly within Oracle Enterprise Manager.

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line, which provides the industry's only complete, integrated and business-driven enterprise cloud management solution. Oracle Enterprise Manager creates business value from IT by leveraging the built-in management capabilities of the Oracle stack for traditional and cloud environments, allowing customers to achieve unprecedented efficiency gains while dramatically increasing service levels.

Only Oracle provides an automated Data masking solution optimized for Oracle databases. This allows organizations to enforce compliance with regulatory requirements such as Sarbanes-Oxley, Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as numerous other laws and regulations that restrict the use of actual customer data.

## Contact Us

For more information about [insert product name], visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.