# IBM InfoSphere Optim Data Masking solution for Oracle E-Business Suite

*Protect the privacy of confidential data in nonproduction environments*

## Highlights

- Protect privacy by de-identifying confidential data across nonproduction environments
- Substitute valid fictionalized values for confidential data and generate accurate results
- Apply application-aware data masking techniques that preserve application integrity
- Leverage prepackaged routines to mask payment card numbers, identifiers and email addresses
- Support compliance with privacy regulations and corporate governance standards

Today's organizations realize that data is a critical enterprise asset, so protecting that data—and the applications holding the data—makes good business sense. However, different types of information have different protection and privacy requirements. Therefore, companies must take a holistic approach to protecting and securing their business-critical information:

- **Discover where the data exists:** You can't protect sensitive data unless you know where it resides across your enterprise and how it is related to other data.
- **Safeguard sensitive data, both structured and unstructured:** Structured data contained in databases must be protected from unauthorized access. File-level data encryption helps make this information unusable or unviewable except to those with valid keys. Unstructured data in documents and forms requires privacy policies to redact (remove) sensitive information while still allowing needed business data to be shared.
- **Secure and continuously monitor access to the data:** Enterprise databases must have real-time insight to ensure data access is protected and audited. Policy-based controls are required to rapidly detect unauthorized or suspicious activity and alert key personnel.
- **Protect nonproduction environments:** Data in nonproduction, training and quality assurance environments needs to be protected against inadvertently revealing sensitive information yet data must still be in usable form during the application development, testing and training processes.

By employing a data protection strategy across all areas and all types of data, organizations can ensure enterprise data is kept secure and protected.

## Ensure privacy compliance—it's the law

Safeguarding the privacy of personally identifiable data is not optional—it's the law. Like all companies, Oracle E-Business Suite sites worldwide are subject to government regulations enacted to protect personal information from misuse. For example, the European Union has established the Data Protection Directive as the framework for privacy protection governing its member countries. In Canada, organizations follow the provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA), while Australian companies are subject to the Privacy Amendment Act. In the United States, multiple regulations apply at the national and state levels. Similar statutes exist worldwide.

Additionally, industry coalitions are developing sector-specific governance standards. For instance, the Payment Card Industry Data Security Standard (PCI DSS), initiated by Visa and MasterCard, is being adopted by other payment card companies in response to the overwhelming incidence of data theft and fraud. The PCI DSS requires members, merchants and service providers to apply 12 security safeguards for the protection of cardholder data.

Oracle E-Business Suite sites use many kinds of confidential data in the course of daily operations—for example, using the Human Capital Management (HCM) application to process employee data for benefits and payroll. In addition to employee identification numbers, names, addresses and telephone numbers, other personally identifiable information includes birth dates, national identifiers (like Canada's social insurance numbers, Italy's Codice Fiscale or the United States' Social Security numbers), bank account numbers, dependents' information, medical information and so on.

## Privacy breaches increase risk and costs

The penalties for failing to protect personally identifiable information can be prohibitive. Corporations and their officers face not only jail time, but also fines that can exceed US$100,000 per incident. In the United States, for instance, the Federal Trade Commission fined ChoicePoint US$15 million for selling sensitive customer data to third parties. Similarly, Capital Financial Administrators (CFA) was fined £300,000 by the United Kingdom's Financial Services Authority (FSA) for failures in its antifraud systems and controls that allowed fraudulent payment requests to client accounts.

Protecting customer privacy engenders public trust and simply makes good business sense. A single privacy breach would be enough for a customer to stop doing business with your company. Without proper controls to protect privacy, your risk for a data breach increases significantly. Consequences include, but are not limited to, loss of market share, brand equity damage, erosion of customer loyalty and lost revenue that can ultimately put your operations out of business.

Oracle E-Business Suite sites acknowledge that protecting data privacy across the enterprise is essential for gaining the trust of customers and business partners. But the sites face many challenges in their efforts to successfully manage personally identifiable information, especially as they move outside the secure transaction processing system.

## Protecting privacy presents challenges

Most sites manage multiple production instances of their Oracle E-Business Suite applications. A company running HCM and Financials, for example, may deploy one application instance supporting its operations in North America; a second for Europe, the Middle East and Asia; and a third for the Asia Pacific region. To support application development, testing, training, backup and other activities, a site may manage anywhere from three to 30 clones for each instance, containing an exact replica of the confidential data from the source system.

Oracle E-Business Suite sites protect private information in their production transaction processing systems by securing and restricting access to underlying data. Strict controls and carefully designed interfaces present a managed view. Unfortunately, it is not so simple to protect private data once it has been copied to nonproduction (development, testing and training) environments, where access controls are more relaxed. In fact, privacy experts maintain that staff such as application developers and testers should have zero access to personally identifiable information. At the same time, developers and testers have unique requirements for interacting with Oracle E-Business Suite data. Specifically, they require access to valid data to accurately test and deploy their Oracle E-Business Suite applications.

Thus the access control methods and managed views used to protect production data simply do not work for development and testing. But using real data could result in a privacy violation or data breach. To resolve the paradox, Oracle E-Business Suite sites need an alternative approach.

## Effective techniques for data masking

Data de-identification is the process of masking or transforming confidential data so that it is safe to use for application development, testing and training. Personally identifiable information is removed from the database.

Transformation algorithms are applied to produce fictional but contextually accurate data, and this information is substituted for the original source data.

As a recognized best practice, de-identifying data provides the most effective way to protect privacy and support compliance initiatives. Data that has been masked or transformed is valid and usable for testing or training. The IBM® InfoSphere™ Optim™ Data Masking solution for Oracle E-Business Suite offers comprehensive, proven capabilities for de-identifying test data, making the data appropriate for testing, but useless to identity thieves and hackers.

InfoSphere Optim offers application-aware data masking capabilities that understand, capture and accurately process Oracle E-Business Suite data elements so that the masked data does not violate application logic. Masked values resemble the look and feel of the original information (see Figure 1). For example, surnames are replaced with random surnames, not with meaningless text strings. Numeric fields retain the appropriate structure and pattern. Checksums remain valid, so that functional tests pass all application validity checks. Most important, InfoSphere Optim propagates all masked data elements accurately and consistently throughout the Oracle E-Business Suite test database, and to other related applications and databases.

InfoSphere Optim provides context-aware, prepackaged data masking routines de-identify key data elements across Oracle E-Business Suite applications: HCM, Financials, Supply Chain and others. InfoSphere Optim provides sophisticated capabilities, including built-in lookup tables for masking names and addresses. Prepackaged routines allow for accurate transformation of complex data elements, such as Social

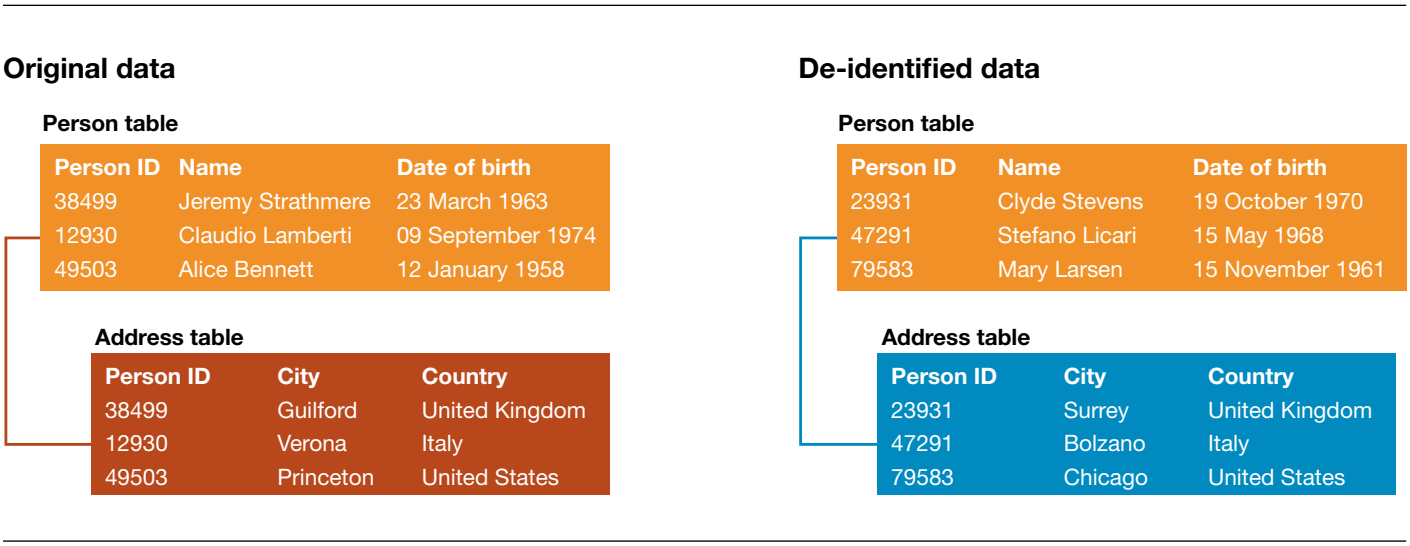


*Figure 1*: InfoSphere Optim data masking capabilities protect privacy across Oracle E-Business Suite applications and databases.

Security numbers, credit card numbers and email addresses. You can also incorporate site-specific data transformation routines, integrating the processing logic from multiple related applications and databases.

InfoSphere Optim is a central data management solution that scales to meet enterprise needs. It provides a consistent approach across the entire family of Oracle applications: Oracle E-Business Suite, PeopleSoft Enterprise, JD Edwards EnterpriseOne, Siebel and all other applications operating on Oracle databases. InfoSphere Optim supports your custom and packaged applications. And it supports all major enterprise databases and operating systems: IBM DB2®, Oracle, Sybase, Microsoft® SQL Server®, IBM Informix®, IBM IMS™, IBM Virtual Storage Access Method (VSAM), Microsoft Windows®, UNIX®, Linux® and IBM z/OS®.

## Quickly identify application data relationships to streamline data masking projects

The InfoSphere Optim Data Masking solution for Oracle E-Business Suite includes prebuilt templates with application logic and validation rules, and understands the data relationships of standard Oracle E-Business Suite modules. However, it's important to understand the entire data model—including customizations—to support masking and other life-cycle activities. Used in combination with the InfoSphere Optim Data Masking solution, IBM InfoSphere Optim Application Repository Analyzer can quickly analyze application metadata to identify relationships in the data models within your Oracle E-Business Suite environment. It identifies application customizations and compares differences in data models across application versions and releases, helping to improve the accuracy and streamline the management of Oracle E-Business Suite application data throughout its life cycle.

## About IBM InfoSphere

IBM InfoSphere Optim is a key piece of the IBM InfoSphere portfolio. IBM InfoSphere software is an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The InfoSphere platform provides the foundational building blocks of trusted information, including data integration, data warehousing, master data management and information governance, all integrated around a core of shared metadata and models. The portfolio is modular, allowing you to start anywhere, and to mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere platform offers an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to help simplify complex challenges and deliver trusted information to your business faster.

## For more information

To learn more about IBM InfoSphere, contact your IBM sales representative or visit: **ibm.com**/software/data/infosphere

To learn more about the IBM InfoSphere Optim Data Masking solution for Oracle E-Business Suite, contact your IBM sales representative or visit: **ibm.com**/software/data/optim/oracle



IBM Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2011


IMS14011-USEN-01