



*Protect the privacy of confidential data  
in non-production environments*

IBM **Information Management** software

## IBM Optim Data Privacy Solution for Siebel Customer Relationship Management

---

### Highlights

---

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

### **Ensure privacy compliance – it's the law**

Safeguarding the privacy of personally identifiable data is not optional – it's the law. Like all companies, Siebel® sites worldwide are subject to government regulations enacted to protect personal information from misuse. For example, the European Union has established the Personal 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 US, 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 Standard requires members, merchants and service providers to apply 12 security safeguards for the protection of cardholder data. In particular, PCI requirement 6.3.4 states that test databases must not contain personal account numbers (PANs) from production data.

### **Privacy breaches increase risk and costs**

Siebel sites process many kinds of confidential data in the course of daily operations. For example, in addition to customer identification numbers, names, addresses and telephone numbers, other personally identifiable information can include birth dates, national identifiers (like Canada's Social Insurance numbers, Italy's Codice Fiscale or US Social Security numbers),

bank account numbers, credit card numbers and e-mail addresses.

The penalties for failing to protect personally identifiable information can be prohibitive. Corporations and their officers face not only jail time, but fines that can exceed \$100,000 per incident. In the US, for instance, the Federal Trade Commission fined ChoicePoint \$15 million for selling sensitive customer data to third parties. Similarly, Capital Financial Administrators (CFA) was fined £300,000 by the UK's Financial Services Authority (FSA) for failures in its anti-fraud 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.

Siebel sites acknowledge that protecting data privacy across the entire system landscape is essential for gaining the trust of customers and business partners. But they face many challenges in their efforts to successfully manage personally identifiable information, especially as it moves outside of the secure transaction processing system.

### **Protecting privacy presents challenges**

Most sites manage multiple production instances of their Siebel CRM applications. A company running Siebel Contact Center and Service, for example, might deploy multiple instances to support its North American, EMEA and APAC operations. To support application development, testing, training, backup and other activities, a site may manage anywhere from 3 to 30 clones for each instance, containing an exact replica of the confidential data from the source system.

Siebel sites protect private information in their production transaction processing systems by securing and restricting access to underlying data by use of authorizations. 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 non-production (development, testing and training) environments, where access controls are less restricted. 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 Siebel data. Specifically, they require access to valid data to accurately test and deploy their Siebel applications.

So, 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, Siebel 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 useable for testing or training. The IBM® Optim™ Data Privacy Solution for Siebel® Customer Relationship Management offers comprehensive, proven capabilities for de-identifying test data, making the data appropriate for testing, but useless to identity thieves and hackers.

Optim's application-aware data masking capabilities understand, capture and accurately process Siebel data elements so that the masked data does not violate application logic. Masked values resemble the look and feel of the original information. For example, country-specific surnames are replaced with random country-specific surnames selected from proprietary lookup databases, not with meaningless text strings. Numeric fields retain the appropriate structure and pattern. Checksums

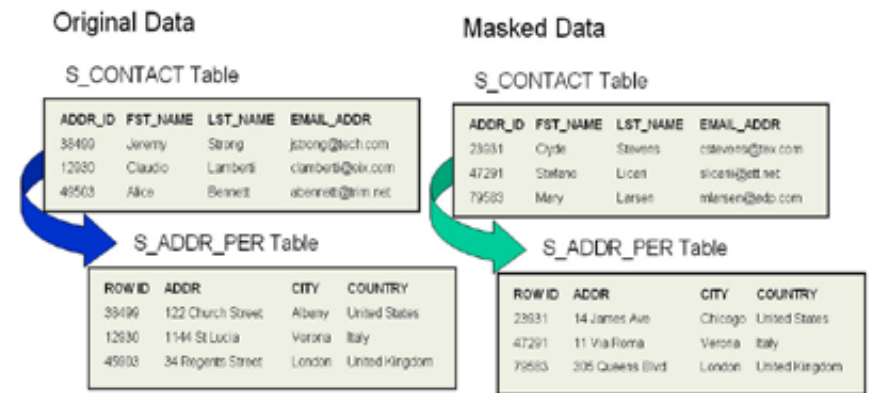


Figure 1. Optim's Key Propagation capability helps preserve the referential integrity, even when data is masked.

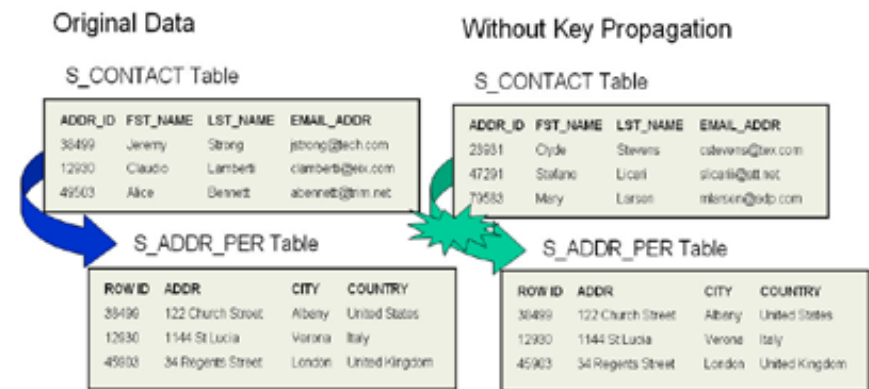


Figure 2. Without a Key Propagation capability, critical data relationships would be severed.

remain valid, so that functional tests pass all application validity checks. Most importantly, Optim propagates all masked data elements accurately and consistently throughout the Siebel test databases, and to other related applications and databases.

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 Security numbers, credit card

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

Optim provides a central data management solution that scales to meet enterprise needs, supporting both 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 VSAM®, Microsoft Windows®, UNIX®, Linux® and IBM z/OS®.

### About IBM Optim

IBM® Optim™ enterprise data management solutions focus on critical business issues, such as data growth management, data privacy

compliance, test data management, e-discovery, application upgrades, migrations and retirements. Optim aligns application data management with business objectives to help optimize performance, mitigate risk and control costs, while delivering capabilities that scale across enterprise applications, databases and platforms. Today, Optim helps companies across industries worldwide capitalize on the business value of their enterprise applications and databases, with the power to manage enterprise application data through every stage of its lifecycle.

### For more information

To learn more about IBM Optim enterprise data management solutions, contact your IBM sales representative or visit: [www.optimsolution.com](http://www.optimsolution.com).



© Copyright IBM Corporation 2008

IBM Software Group  
111 Campus Drive  
Princeton, NJ 08540-6400  
USA  
[www.optimsolution.com](http://www.optimsolution.com)

Produced in the United States of America  
05-08  
All Rights Reserved

DB2, IBM, the IBM logo, IMS, Informix, Optim, VSAM and z/OS are trademarks or registered trademarks of the IBM Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Windows and SQL Server are registered trademarks of Microsoft Corporation in the United States and other countries. All other company or product names are trademarks or registered trademarks of their respective owners.

References in this publication to IBM products, programs or services do not imply that IBM intends to make them available in all countries in which IBM operates or does business.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.