

**Mastering Employee Resource Management
with Oblix NetPoint:
Achieving Core Business Objectives through
Effective Identity Management**

W H I T E P A P E R



Copyright © 2003 Oblix, Inc. All rights reserved.

This white paper is for informational purposes only. Oblix makes no warranties, expressed or implied, in this document. Mention of third-party products within this publication is for informational purposes only and constitutes neither an endorsement nor a recommendation.

The information contained in this document represents the current view of Oblix on the issues discussed as of the date of the publication. Because Oblix must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Oblix, and Oblix cannot guarantee the accuracy of any information presented after the date of publication.

Software and documentation Copyright © 1996-2003 by Oblix, Inc. All rights reserved. Oblix, NetPoint, Oblix NetPoint, and the Oblix logo are registered trademarks of Oblix, Inc. NetPoint COREid System: User Manager, Group Manager, Organization Manager, IdentityXML, Certificate Processing Server (VeriSign®), COREid Server, and WebPass; NetPoint Access System: Access Manager, Access Server, WebGate, and AccessGate; COREid, FEDERATEDid Layer, Oblix IDLink, Associate Portal Services, NetPoint System Console, NetPoint Ready Realm, NetPoint Federation Services, NetPoint Mainframe Security Connector, NetPoint SAML Services, and their logos are trademarks of Oblix, Inc. All other company and product names are trade names, service marks, trademarks or registered trademarks of their respective companies.

Printed in the United States of America.

Printing Date: July 2003

Part Number: obx63a

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
T 408.861.6800 F 408.861.6810

European Headquarters
Atrium Court
The Ring, Bracknell
Berkshire RG12 1BW, UK
T +44(0)1344 393 054

www.oblix.com

Executive Summary	1
Key Objectives in Today's Employee Resource Management Initiatives	2
The Role of Identity Management	3
Leading Corporations Turn to Oblix NetPoint	4
Increasing Employee Productivity and Experience at A Large Fast-food Chain	4
Large Telco Provider Meets Compliance with Oblix NetPoint	5
Reducing the Time and Cost of IT Administration at i2 Technologies	7
Driving Real Business Results	9

Executive Summary

Large companies across multiple industries are struggling to leverage one of their greatest assets — the sizable workforce that sells to and supports customers. Retail, food, and service leaders succeed by building strong relationships with their employees, educating them to deliver a consistent corporate message, and training them to provide a uniform customer experience through best practices, even in the face of high turnover. In other industries, like healthcare, financial services, and telecommunications, companies are required to demonstrate compliance with regulatory requirements dealing with safeguarding corporate data and resources. Understanding and managing employee access to different systems and data is key to lowering risk of non-compliance. Of course, all of these firms share a need to improve the efficiency of administering the systems that hold and manage employee profile information.

These companies share a common challenge in managing identity data to enable their employees to do their jobs and be more productive. This paper discusses how companies with large numbers of employees in multiple geographic locations or companies facing regulatory requirements (e.g. HIPAA or Sarbanes-Oxley) can utilize Oblix Identity Management solutions to increase productivity, lower administration costs, and decrease risk of non-compliance.

Business managers who are struggling to improve employee productivity and service delivery, particularly in high-turnover environments, should read on to find how one of the largest fast-food chains is standardizing customer experience and best practices across its many locations with Oblix NetPoint®.

Executives who are concerned about new financial and data integrity regulations such as Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley will be interested in how one of the largest wireless operators in the U.S. is using Oblix NetPoint to strengthen its audit compliance and reporting capabilities.

Finally, IT managers who are seeking to cut IT administration time and costs as well as redirect resources toward strategic initiatives will benefit from the experience of i2 Technologies in automating its processes for managing employee profiles across all enterprise systems with Oblix NetPoint.

Key Objectives in Today's Employee Resource Management Initiatives

Identity Management issues cut across industries and geographical regions. Wherever they operate and however they model their business, most large companies share several common business objectives:

- **Improve Employee Productivity and Service Delivery**

In some industries, high turnover requires uniform business processes and training to ensure a strong brand, a common corporate culture, and a familiar customer experience across locations. In other industries, firms have reduced headcounts to align expenses with the business conditions. For employees, this often means more work with less available time. For employers, this increases the value of remaining employees and, in turn, increases the need to make those employees more productive and satisfied with their jobs and the company. In any industry, employees want to spend their available time doing productive work, and employers want to increase effectiveness of internal communications about operations and strategy. Benefits of success here include higher ROI, lower turnover costs, and increased competitiveness in the marketplace.

- **Ensure Security and Compliance**

Particularly in the last year, regulatory changes in the business and regulatory environment have increased every firms' need to ensure that sensitive information is protected, while at the same time providing audit records of access, permission and identity changes. Companies have come to understand that information security risks come not only from external users, but often from internal users too. As the employee base increases, so does the risk of improper access. Information security has become more than a technology problem and is now a key business issue, as executives and their boards understand their responsibility and accountability in information security governance. Regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley increase requirements for managing access and distribution of financial and customer data. As a result, managers are struggling to understand risks from within, and are actively seeking methods for centralizing identity, access, and audit controls. Some benefits of success in this area are obvious; managers avoid litigation costs and regulatory penalties. Less obvious benefits are also important; firms that successfully manage information security become trusted partners, vendors, and employers.

- **Cut Time and Cost of IT Administration**

Employee-related IT administration brings some necessary cost. Maintaining accounts in corporate systems, resetting passwords, and provisioning new access rights all require administrative time. Companies with large numbers of employees spend a larger amount of time and cost administering employee accounts. Even

worse, many of these businesses experience high turnover, thereby increasing the administrative burden. Each lost employee, as well as that employee's replacement, requires account maintenance or closure, address updates, etc. For large firms, identity administration across the corporate IT environment can bring significant costs. The benefits of successfully managing identity administration include lower costs, but also increased opportunity, as resources can be deployed toward new business initiatives instead of routine tasks.

The Role of Identity Management

The broad objectives discussed in the previous section can be applied to a variety of business scenarios. However, many companies have found that Identity Management is at the core of multiple business initiatives, and can "make or break" key applications. It is useful, therefore, to look at how the above business objectives impact Identity Management requirements.

For example, when viewed through the Identity Management lens, improving employee productivity and service delivery requires:

- Personalized views through corporate portals or intranets
- Automatic access to corporate applications, best-practice documents, training systems, etc.—tailored to title, department, or job code
- Reducing the number of login steps, IDs and passwords required to give employees access to key data

Viewed the same way, ensuring security and compliance requires:

- Centralized management of disparate security policies and practices across different applications
- A common view of employee profiles and their related access policies
- Audit trails of application access and identity profile changes
- Automation of security and identity-related business processes

Finally, cutting the time and cost of IT administration requires:

- Automation of repetitive processes such as password reset, adding new users, and provisioning accounts
- Delegating authority for Identity Management to the appropriate level
- Processing new-user and departing-user account management in minutes instead of days

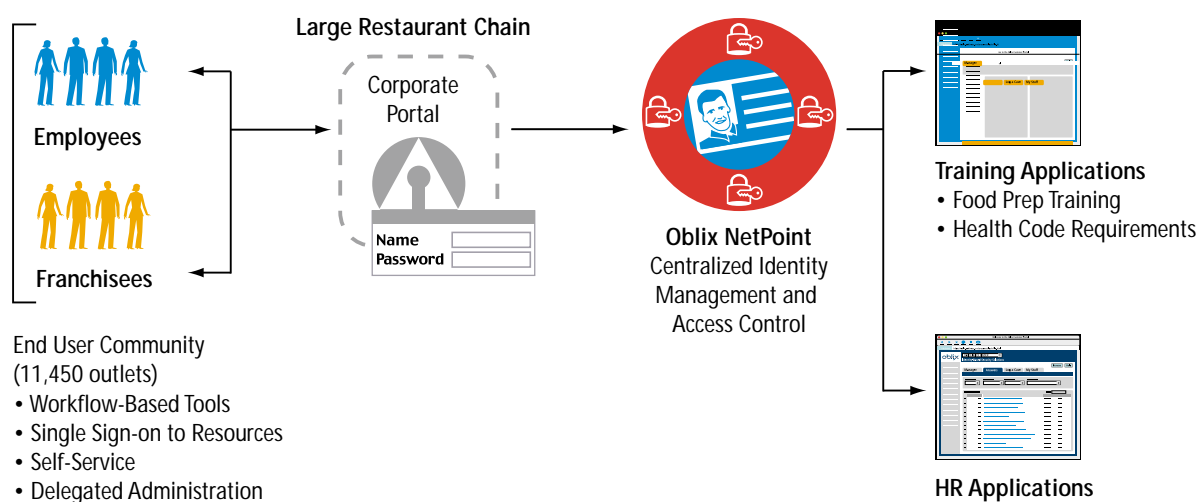
Leading Corporations Turn to Oblix NetPoint

Many global corporations are already enjoying the benefits of an Identity Management solution. Oblix customers including Southwest and i2 Technologies have streamlined their IT processes, improved employee productivity, and increased confidence in their ability to comply with regulations. Each of these firms has deployed Oblix NetPoint to meet the business objectives described above.

Increasing Employee Productivity and Experience at A Large Fast-food Chain

One of the largest fast-food chains in the United States was able to use Oblix NetPoint to support a key business initiative to deliver consistent products, services, and customer experience throughout its many restaurants. Like many franchise-based service firms, fast-food restaurant chains are highly competitive and must manage high employee turnover as well as disparate geographic locations. Building a common culture requires strong processes to bring new hires up to speed on culture and practice quickly, as well as providing franchise owners with accurate and consistent product and operations data.

The fast-food chain chose to implement an employee and franchisee portal on top of its internal SAP enterprise system. The SAP portal relies on Oblix NetPoint to perform Identity Management for all users of the portal, across the United States. NetPoint provides a framework for centrally managing user information, which can be leveraged to deliver applications to the appropriate employees consistently across the entire



The fast-food chain's employee portal connects thousands of employees to the corporation, strengthening culture and supporting best practices

corporation. This allows for new employees to become productive quickly and for more experienced employees to learn new skills and feel more connected with the organization. For the fast-food chain, this combination has resulted in a closer relationship with employees, a stronger culture, and greater productivity, ultimately reflected in an overall improvement in customer experience and service operations.

Specific Oblix NetPoint product features used by the fast-food chain to support a common employee experience and uniform service delivery within a high-turnover, multi-location environment include:

- **Automated Workflow** to ensure that common business processes in the hiring and firing of employees are followed.
- **Single Sign-on** to reduce the number of logins that employees have to remember.
- **Self-Registration** and Service to enable employees to manage aspects of their own identity profiles. For example, many companies struggle to manage address changes when sending out W2 forms, and Oblix NetPoint's self-service functions eliminate wasted time and re-work.
- **Delegated Administration** to allow franchise managers to create and deactivate users in a centralized system.

Large Telco Provider Meets Compliance with Oblix NetPoint

A large global telecommunication and wireless provider found that with tens of thousands of employees across the globe, ensuring confidentiality and securing key data was a challenge. Specifically, many of the firm's corporate applications had their own security models and access control. As a result, the firm had no single point of management and reporting for enterprise-wide employee data access. Regulations such as Sarbanes-Oxley required a level of certification that was impossible without a centralized set of access and Identity Management policies.

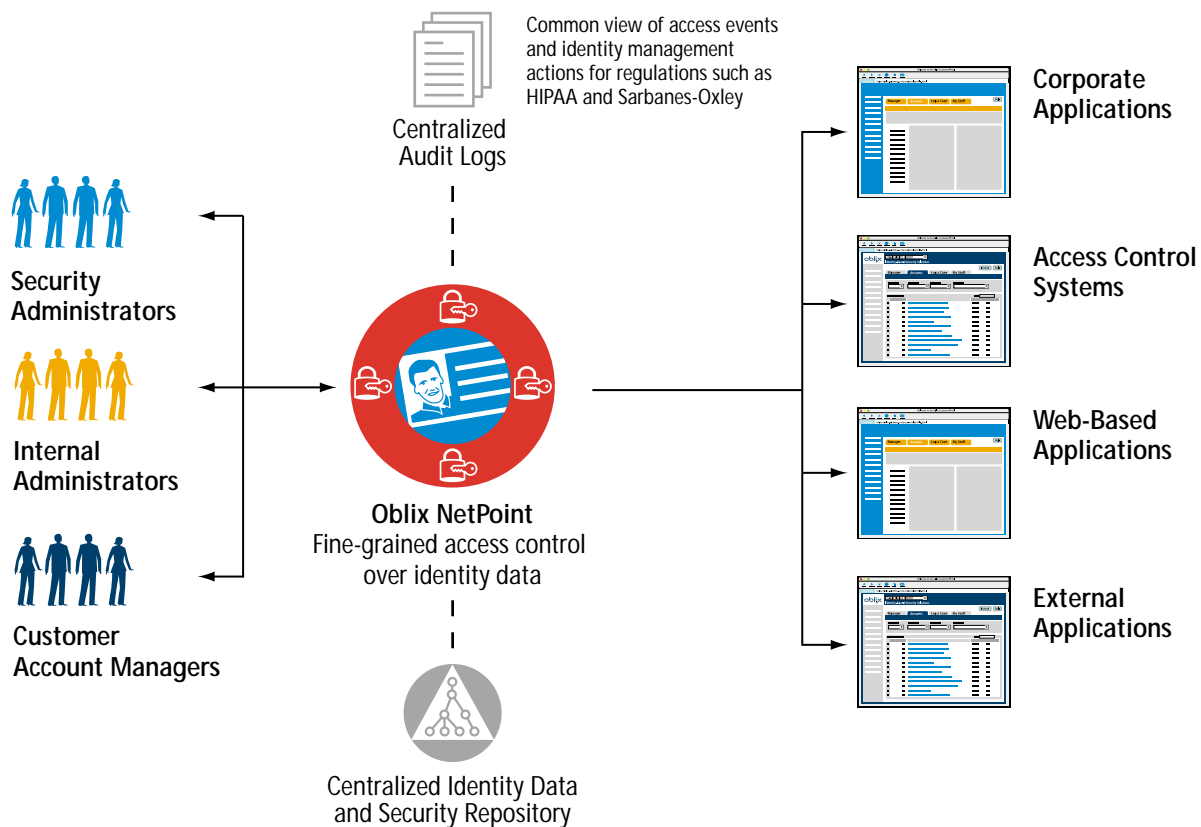
The company chose Oblix NetPoint to address this requirement. With NetPoint, the wireless provider created a single layer for managing security policies, separate from the applications that used the policies. The benefit to the firm was twofold: first, it decreased compliance risk through a single point of management control, and second, it decreased application development time by eliminating application-specific identity and access management functionality.

"A standard audit was performed, and we found we had no way of centralizing the administration of our security. As a publicly traded company, we are required to safeguard our assets, and Oblix will help us do that."

— Large Telecommunication and Wireless Provider

Specific Oblix NetPoint product features used by this wireless provider to ensure security and compliance include:

- **Auditing and Logging** to permit tracking and reporting of each identity change and authentication and authorization success or failure.
- **Access Testing** to show which users are allowed to access each application.
- **Attribute Access Control** to provide fine-grained control over who can view and modify individual identity attributes.
- **Delegated Administration** to provide centrally defined administrative controls over the user and group administration.
- **Automated Workflow** to allow specific business processes to be applied to identity change and user administration events.



A global wireless provider relies on Oblix NetPoint to centralize management and auditing of security and access policies

Reducing the Time and Cost of IT Administration at i2 Technologies

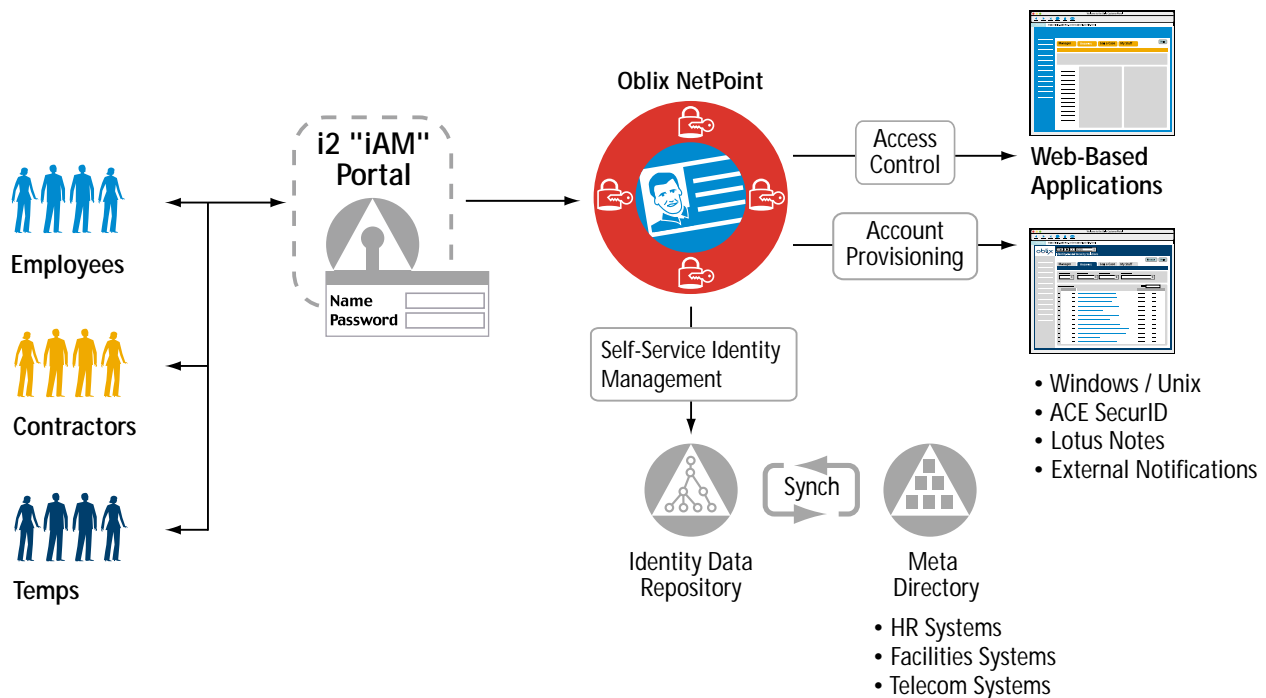
Employee identity information can be highly dynamic, and large organizations with even moderate turnover are faced with managing identity information throughout each employee's life cycle. These identity events include managing new hires, location changes, promotions, name changes, leaving the company, retirement, as well as other organization specific events. Some organizations are faced with large seasonal effects such as new student registration or distribution of W2 forms at tax time. In many cases, identity changes must be propagated across multiple systems such as the corporate directory, email systems, applications, mainframes, etc. Keeping data consistent across systems often requires tremendous manual update, error correction, and re-work.

For one large software vendor, i2 Technologies, data integrity issues prevented efficient management of employee information. The firm has approximately ten different data sources, each holding different pieces of an individual's identity. For example, the email server might hold an employee's email address, while the HR application stores his name and address, but not necessarily desk location. The telecom system stores his phone number, and so on. Identity Management gives i2 an aggregated view of each individual, as well as an automated way to manage this information as employees are hired, promoted, or leave the company.

One benefit of installing Identity Management within such an environment has been significant reduction in time spent administering user data. For example, since installing Oblix NetPoint, calls to the internal help desk for password reset and lost password issues have dropped over 70%, leaving staff to concentrate on more strategic issues. Layered over the various user data stores, i2's "I AM" portal provides employees, contractors, and temporary workers with a single starting point for self-service account management of their identity information. This drastically reduces support costs on mundane tasks and eases administration complexity and overhead. According to John Frazier, Director of All Operations at i2, "Without a solid Identity Management infrastructure, you'll be making access decisions on bad data...and this is worse than making no decisions at all."

Specific Oblix NetPoint product features used by i2 to cut the time and cost of IT administration include:

- **Delegated Administration** to push administrative tasks down to the employees or managers closest to the source.
- **End User Self-Service** to allow employees to manage their own identity profile based on permissions.
- **Password Reset and Lost Password** functions to eliminate help desk calls.
- **Automated Workflow** to streamline the processes associated with employee lifecycle events.
- **Powerful Group Management** functions to facilitate creation of dynamic work groups based on attributes such as title and department, drastically simplifying administration.



i2 Technologies relies on Oblix NetPoint to automate the process of user information management, system access, and identity data synchronization

Driving Real Business Results

Regardless of product, service, industry, or location, every large company today understands the value of productive employees that are loyal, informed, and provide excellent and consistent service to customers. Such benefits do not come by accident; leading firms that are known for this type of workforce have not only built best practices, but also a means to connect employees with information about these practices. For service leaders such as Southwest Airlines, employee resource management is a core driver of business success and a competitive weapon, not an afterthought. Corporations such as these have implemented powerful Identity Management solutions, built on Oblix NetPoint.

Using Oblix NetPoint to drive internal and external facing portals, these firms benefit from knowing that employees have consistent access to the information and applications they need to do their jobs, while managers retain centralized reporting and auditing of this access, to meet corporate and government regulations. The result of this investment is improved service and productivity, lower security risks, and significantly lower time and cost of administration.