

An Oracle White Paper
August 2010

Massachusetts Data Security Law Signals New Challenges in Personal Information Protection

Introduction	2
Massachusetts Data Protection Law.....	3
First of its Kind.....	3
High Risk to Enterprises	4
Uncertain Future.....	4
Massachusetts 201 CMR 17.00 Requirements.....	5
The Challenge for Enterprises	6
Failure of Manual Controls.....	6
All-Encompassing Data Security.....	7
Oracle’s Total Security Portfolio.....	8
Encryption	11
Requirements and Difficulties	11
Oracle’s Single Encryption Solution	12
Privileged User Accounts.....	13
How Massachusetts Law Applies	13
Hard to Control	14
Oracle Manages Privileged Accounts	14
Access Control’s Vital Role.....	16
201 CRM 17.00 Access, Authorization and Authentication	16
Access Control Challenges.....	16
A Program That Works	17
Oracle Identity Management.....	18
Fraud Control	19
Conclusion	19

Introduction

State data protection laws have already had a profound impact on enterprise security programs, effectively covering the personally identifiable information (PII) of most U.S. citizens and obliging corporate security and compliance officers to adopt broad programs to safeguard customer data.

The Massachusetts data protection law, 201 CMR 17.00, could have the most profound impact of all. The law, which recently went into effect, goes far beyond previous state mandates, in requiring companies to have comprehensive information security programs in place.

This goes well beyond the more than 40 existing state data breach notification laws. In the absence of federal legislation, which has languished in various iterations in Congress for years, state data breach notification laws, starting with California's milestone SB 1386, marked a turning point in corporate data protection requirements. The law effectively became national, as almost every company doing business online conducts transactions with California residents and stores their PII.

The rapid adoption of very similar laws in most states reinforced the need to protect *all* customer data, as potential breaches would likely affect far more people. This had significant ramifications in terms of the cost of disclosure: the actual cost of notification; free credit reports and in some cases anti-fraud protection programs for customers; remediation measures, including adding security technology, and correcting flawed policies and procedures that may have contributed to the breach, and brand reputation damage.

The laws were an important factor in the implementation of many new security measures, particularly driving the adoption of data encryption, from back-end databases to laptops and removable storage media. This is a consequence of the general exemption of encrypted data from the notification requirements.

The data breach notification laws are apparently just a start, as states are beginning to become more and more involved in data protection requirements and enforcement. For

example, one of the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) gives state attorneys general the power to file suit over HIPAA violations in their jurisdiction, dramatically increasing the oversight in what has generally been an enforcement vacuum over the years. Also, Nevada and New Hampshire now require PCI DSS compliance by law, so companies who handle credit card transactions with residents of those states must be answerable to them as well as the card-issuing companies.

The Massachusetts law, however, takes the state role in data protection to a new level.

Massachusetts Data Protection Law

First of its Kind

Massachusetts 201 CMR 17.00 is the first state law to require companies to have a data protection program in place to protect PII of its residents and be prepared to attest to its use in the event of an investigation of a possible compromise.

This goes far beyond the data breach disclosure laws which deal with the consequences of lost or stolen data, but don't require protection programs or attempt to delineate what such programs should include, except indirectly by providing a safe harbor for encrypted data. The law potentially covers all types of businesses: in state, out of state, large enterprises and SMBs, and across most verticals.

Unlike the sundry data breach disclosure laws, which are more or less the same—mandatory disclosure; exemption if data is encrypted—201 CMR 17.00 mandates a comprehensive data protection program, including encryption, access control, authentication, risk assessment, security policies and procedures, security monitoring and training. In addition, similar to the provisions of HITECH, third-party service providers are required by contract to protect PII.

This must be in the form of a formal, “comprehensive” written information security program, generally referred to as a WISP. In the event of an investigation or enforcement action, companies must produce the document, show that it covers all the areas spelled out in the law and be prepared to demonstrate that the program is real and not just paper. The WISP should include “appropriate technical, administrative and physical safeguards” to protect PII. It is good practice to have such a program to protect against violations of the many state data breach notification laws, but those simply give you the option of encrypting the data or suffer the consequences if you experience a breach.

High Risk to Enterprises

Enterprises will be held to a higher standard than smaller businesses, as the law states that the security program be appropriate to the size and resources. Larger businesses can expect more severe penalties if their programs are deemed deficient or procedures lax, though precedents and guidelines will be established by the actions of the attorney general in the first sets of cases.

So we can expect the standards to which companies will be held accountable will depend on the safeguards laid out in the law, which are required to be appropriate to:

- The size, scope and type of business
- The amount of resources available
- The amount of stored data
- The need for security and confidentiality of both consumer and employee information

It is most likely that penalties will depend on the nature and scope of the violation, the degree to which the company made a good faith effort to comply and the size and resources of the offending organization. Companies that demonstrate that they are diligent in following a comprehensive and appropriate WISP should expect to fare better in the event of a breach than those that do not.

The cost could be staggering. Companies can be fined up to \$5,000 per compromised record. There is no provision for audit; oversight will come through the attorney general's office in the event of actions and investigations. So, if PII that includes Massachusetts is compromised in any way, companies have to be prepared to present and defend their data protection program.

Uncertain Future

It remains to be seen how aggressive the Massachusetts attorney general's office will be in bringing actions against companies operating both inside and outside the state, but the other shoe that is waiting to drop is whether other states will follow suit, as they have en masse in the wake of California's data breach notification law, and enact their own data protection legislation. The implications could be enormous. Corporate exposure would increase and a single data breach could result in multiple actions and possible penalties in multiple state jurisdictions. Imagine the compromise of a database of PII of customers from every state in the country if 30 or 40 states have laws that require, like Massachusetts, comprehensive data protection programs, and provide for monetary penalties for each record involved.

Moreover, unlike the "one size fits all" breach notification statutes, subsequent state data protection laws may and likely will vary widely, perhaps setting more stringent and proscriptive policy and procedure requirements. Some might require companies to implement specific security technologies or to file written information security programs with the attorneys general and or periodic audit reports.

Enterprises' best course is to examine their information security programs and assure that they are sufficiently inclusive to cover the strictest possible state requirements that may arise. Mid- to large-sized enterprises should expect the strictest interpretations of 201 CMR 17.00 requirements and those of any similar, future state laws and that they will be held to high security standards – and subject to the heaviest penalties-- in the event of enforcement actions.

Massachusetts 201 CMR 17.00 Requirements

The law spells out two sets of requirements for the required information security program. The first outlines the duties and standards for protecting PII. These include:

- Employee compliance with policies and procedures
- Means for detecting and preventing security system failures.
- Developing security policies controlling the storage, access and transportation of records containing PII outside of business premises.
- Preventing terminated employees from accessing records containing PII.
- Requiring such third-party service providers by contract to implement and maintain appropriate security measures for personal information
- Regular monitoring to prevent unauthorized access to or unauthorized use of personal information
- Reviewing the scope of the security measures at least annually
- Documenting actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken

From a more technical perspective, the law specifies computer system requirements, which include, “to the extent technically feasible:

- Secure user authentication protocols that shall encompass:
 - Control of user IDs and other identifiers
 - A reasonably secure method of assigning and selecting passwords, or other authentication technologies , such as biometrics or tokens
 - Control of data security passwords in a location and/or format that does not compromise the security of the data they protect
 - Restricting access to active users and active user accounts
- Secure access control measures that:
 - Restrict access to records and files containing personal information to those who need such information to perform their job duties
 - Assign unique identifications plus passwords to each person with computer access

- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly
- Monitoring of systems for unauthorized use of or access to personal information
- Encryption of all personal information stored on laptops or other portable devices
- Up-to-date firewall protection and operating system security patches
- Up-to-date malware protection
- Education and training of employees on the proper use of the computer security system and the importance of personal information security

The Challenge for Enterprises

Failure of Manual Controls

Enterprises are typically subject to multiple federal, industry and state security mandates, but the introduction of 201 CMR 17.00 cuts across all sectors. The specter of multiple states enacting their versions of data protection laws, each with the potential for their own policy, practice and technology requirements, raises the stakes and exacerbates the collective complexity of the regulatory environment.

Accordingly, organizations should adopt information security policies, processes and procedures that not only meet the Massachusetts requirements, but should be sufficiently flexible and nimble enough to encompass data protection laws that may be passed by other states. Further, enterprises must have solutions in place that can demonstrate their diligence conclusively in that their security program's policies and technical controls were in effect in the event of a violation allegation and enforcement action.

The environment has grown far too complex to rely on manual data security and access control processes, which may have been adequate in simpler times. The exponential increase in information created, transmitted and stored in large, distributed organizations, the maize of Internet-connected mobile and remote employees, partners, suppliers and customers, and the pervasive, sophisticated criminal threat have largely outstripped enterprises' ability to implement and reasonably manage flexible, reliable, enforceable and auditable data security programs in a manual fashion.

Data security and access control programs that rely heavily on manual processes and procedures are both labor-intensive and largely ineffective. They become bottlenecks and business inhibitors that are likely to be circumvented in practice as business managers eschew cumbersome security

procedures to “just get it done.” Documentation and reporting for forensics, audit, litigation and enforcement is at best difficult and requires many dedicated man hours. Typically, there are gaps in implementation and documentation, and manual processes are prone to human error, undermining security and, in many cases, business operations. Real-time or even regular activity monitoring is all but impossible.

On the other hand, automated security tools, such as Oracle’s comprehensive suites of data security and identity management products, help translate policies and procedures into a practical, sustainable, continuous and auditable data protection program.

All-Encompassing Data Security

A comprehensive data security program, supported by robust automated tools, will protect the business and its customers on the one hand, and meet the requirements of the new Massachusetts law, especially for large organizations that will be expected to devote substantial resources to protect customer and employee information. The program should be both broad and deep enough to meet the potential range of requirements if more states enact their own information security laws.

Data security begins “close in,” with the data itself, and extends out to tightly controlled data management, and granular and manageable access controls that both empower the business and meet stringent security and regulatory requirements. At its foundation, a comprehensive data security program should focus squarely on:

- Strong data protection in the form of seamless encryption through the entire information lifecycle. Encryption should be transparent and reasonably easy to manage.
- Well-defined role-based database and applications access controls, in particular, privileged user controls and clearly delineated separation of duties for those privileged users. Privileged users are often poorly defined, and poorly managed. Organizations can quickly lose control over who can grant or deny access and even change or create databases.
- Database activity monitoring, particularly privileged user activity. Left undetected, unauthorized database access and/or administrative actions invalidate security policies and leave enterprises vulnerable.
- Centrally managed access controls that limit user authorization and access to applications, systems and information strictly on business need. Access is typically managed on an individual system/application basis, creating management inefficiency and poor security controls born of unnecessary complexity and multiple user IDs and passwords.

- Granular, automated role-based provisioning and de-provisioning of users and user authorization. Typically, administrators and business managers err on the side of excessive privilege, rather than risk impeding the business by not granting sufficient authorization.
- Continuous user access monitoring. This is critical for security, assuring that users are not exceeding their authorization and are indeed who (or what) they say they are. This is also critical from a compliance perspective, as continuous monitoring—as opposed to a snapshot check or spot sampling—demonstrates that controls are being enforced.
- Appropriate authentication for each asset access/usage. Helps assure that the user is who he says he is and allows for strength of authentication according to user role and responsibility (e.g., office assistant or systems manager?) and the criticality and/or sensitivity of the assets.
- Flexible and thorough audit/reporting capabilities. Detailed and customizable audit and operational reports are essential for compliance, forensics and validation of the effectiveness of security controls.

Oracle's Total Security Portfolio

Oracle provides end-to-end protection, with comprehensive data security and identity management tools.

Oracle's comprehensive database security portfolio, including *Oracle Advanced Security*, *Oracle Data Masking*, *Oracle Database Vault*, *Oracle Database Firewall* and *Oracle Audit Vault*, protects PII by providing transparent data encryption, masking, privileged user and multi-factor access control, as well as monitoring of inbound SQL traffic and database activity.

Oracle Access Manager, *Oracle Identity Manager*, *Oracle Identity Analytics*, *Oracle Identity Federation* and other products in the suite of Oracle identity management solutions provide application and system-level security, giving enterprises the tools they need to create and sustain a centrally managed, automated and auditable access control program.

These tools provide the essential capabilities that enable enterprises to transform unwieldy manual processes and policies that are difficult to enforce and validate, into highly automated, granular and scalable security programs. This caliber program, incorporating the essential steps and components outlined above, will ensure a strong corporate security posture and compliance with Massachusetts 201 CRM 17.00 and the potential state laws to follow. We'll examine these steps and components in some detail.

ORACLE PRODUCT FOR MASSACHUSETTS 201 CRM 17.00	
17.03: DUTY TO PROTECT AND STANDARDS FOR PROTECTING PERSONAL INFORMATION	
EVERY COMPREHENSIVE INFORMATION SECURITY PROGRAM SHALL INCLUDE:	ORACLE PRODUCTS
<p>Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic...records including:</p> <ul style="list-style-type: none"> • Employee compliance with policies and procedures; • Means for detecting and preventing security system failures. 	<p><i>Oracle Database Vault</i> monitors and enforces privileged user access and monitors database activity to assure policy compliance. Establishes and enforces separation of duties.</p> <p><i>Oracle Database Firewall</i> monitors inbound SQL traffic for unauthorized SQL commands, including malicious SQL*Injection threats.</p> <p><i>Oracle Audit Vault</i> reports and alerts</p> <p><i>Oracle Access Manager</i> facilitates centralized policy control, enforces access, authorization and authentication policies and rules. Monitors access activity and provides report data for forensics, audit and compliance.</p> <p><i>Oracle Identity Manager</i> detects "ghost" account activity</p>
Preventing terminated employees from accessing records containing personal information	<i>Oracle Identity Manager</i> automates de-provisioning of terminated employees and detects "ghost" account activity
Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.	<ul style="list-style-type: none"> • <i>Oracle Database Vault</i> • <i>Oracle Audit Vault</i> • <i>Oracle Access Manager</i> • <i>Oracle Identity Manager</i> • <i>Oracle Adaptive Access Manager</i> detects fraud activity
Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information	<ul style="list-style-type: none"> • <i>Oracle Audit Vault</i> • <i>Oracle Access Manager</i>
17.04: Computer System Security Requirements	
Secure user authentication protocols including:	
<ul style="list-style-type: none"> • Control of user IDs and other identifiers 	<ul style="list-style-type: none"> • <i>Oracle Access Manager integrates with leading authentication providers and provides centralized policy-based, tiered authentication management</i> • <i>Oracle Identity Analytics provides fine-grained role-based access control</i> • <i>Oracle Identity Manager</i> • <i>Oracle Database Vault</i>
A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as	<ul style="list-style-type: none"> • <i>Oracle Access Manager</i>

biometrics or token devices	<ul style="list-style-type: none"> • <i>Oracle Identity Manager</i> • <i>Oracle Database Vault</i>
Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect	<ul style="list-style-type: none"> • <i>Oracle Database Vault</i> • <i>Oracle Access Manager</i> • <i>Oracle Adaptive Access Manager</i>
Restricting access to active users and active user accounts only	<ul style="list-style-type: none"> • <i>Oracle Identity Manager</i> • <i>Oracle Access Manager</i>
Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system	<ul style="list-style-type: none"> • <i>Oracle Access Manager</i> • <i>Oracle Adaptive Access Manager</i> • <i>Oracle Database Vault</i>
Secure access control measures that:	
Restrict access to records and files containing personal information to those who need such information to perform their job duties; and	<ul style="list-style-type: none"> <i>Oracle Access Manager</i> <i>Oracle Identity Manager</i> <i>Oracle Identity Analytics</i> <i>Oracle Database Vault</i> <i>Oracle Database Firewall</i> <i>Oracle Advanced Security</i>
Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls	<ul style="list-style-type: none"> <i>Oracle Access Manager</i> <i>Oracle Identity Manager</i> <i>Oracle Database Vault</i>
Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly	
Monitoring of systems, for unauthorized use of or access to personal information	<ul style="list-style-type: none"> <i>Oracle Database Vault</i> <i>Oracle Database Firewall</i> <i>Oracle Audit vault</i> <i>Oracle Access Manager</i> <i>Oracle Identity Manager</i> <i>Oracle Adaptive Access Manager</i>

Encryption

Requirements and Difficulties

Unlike state data breach disclosure laws, which exempt lost or stolen data from the notification requirements if it is encrypted, the Massachusetts law requires data encryption. Furthermore, 201 CRM 17.00 addresses one of the loopholes in data breach disclosure laws: Encryption is useless if the encryption keys are compromised. Note the law's definition of "breach of security" as:

"The unauthorized acquisition or unauthorized use of unencrypted data or, *encrypted electronic data and the confidential process or key* that is capable of compromising the security, confidentiality, or integrity of personal information...that creates a substantial risk of identity theft or fraud...."

At one time, enterprises generally avoided encryption, despite its obvious security benefits, because of deployment and management difficulties and insecure implementations. Native or home-grown encryption solutions typically don't scale well for the enterprise, and companies have been hard-pressed to find a single, well-implemented solution that addresses data at rest, in motion and backups.

Enterprises can no longer avoid encrypting sensitive data. Regulatory mandates such as 201 CRM 17.00, data breach disclosure laws HIPAA/HITECH and PCI DSS have made data encryption a security imperative. Enterprises are now obligated to deploy an encryption solution that is secure, scalable and easy to manage.

The Massachusetts data protection law doesn't go into detail about the type of encryption to be used or how it is to be implemented, but it is clear that the intent of the law is to encrypt data in a way that is sustained through the information lifecycle, wherever it is:

"Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."

It follows, then, that data must be seamlessly and automatically encrypted and protected at rest and in transit until it is accessed by an authorized user to prevent exposure and violation of the law. Data should be protected in transit through organization's encryption technology of choice or secure transport technologies such as SSL/TLS.

Key management is the critical piece that assures that information can be accessed only by authorized user. And it has historically been the issue that has derailed encryption projects and/or rendered them ineffective, and often fails because issuance, storage and renewing are difficult.

Key management is hard to implement: The result is typically lax controls, which give too many people potential access to data. Poor key management can also result in lost keys that can render data inaccessible, interrupting business and wasting IT resources. In the worst-case scenario, data may be irrevocably lost. It's hard to properly protect and manage keys while maintaining ease of use necessary to the business.

The frequent result is that key management becomes a hallow security control, as IT managers give way to more pressing priorities and pressure from the business side to relax key management controls. As a consequence, keys become widely available to multiple users, rendering encryption ineffective.

Oracle's Encryption Solution

Oracle Advanced Security provides comprehensive encryption capabilities in a single seamless product, encrypting data in storage, in transit and backup. In addition it provides strong authentication as an alternative to passwords.

Oracle Advanced Security TDE encrypts data when written to disk and decrypts it after a user has been successfully authenticated. After authentication to the database the user must also pass any access controls enforced by the application and database. TDE prevents attempts to bypass the database and access sensitive data directly at the operating system layer. TDE supports transparently encrypting specific sensitive columns with TDE column encryption or encrypting entire applications with TDE tablespace encryption. Using Oracle Enterprise Manager, a column can be quickly and easily encrypted or an entire encrypted tablespace can be created to store all application tables. In addition to using Oracle Enterprise Manager, both column encryption and tablespace encryption can also be enabled using SQL commands. TDE integrates with Oracle RMAN enabling encryption of entire database backups. Previously used master keys are retained in the Oracle Wallet for recovery purposes. TDE also can be used with Oracle Data Pump to encrypt data export from the Oracle database to a flat file.

Oracle Advanced Security addresses encryption's biggest impediment with built-in key management. The transparent data encryption (TDE) feature automatically creates data encryption keys behind the scenes and protects those encryption key with another key known as the master key. This two-tier system provides an elegant solution that protects the data encryption keys. The master key securely stored outside of the database, in an Oracle Wallet, a PKCS#12 formatted file, which is password-encrypted. The master key can alternatively be stored in a network attached hardware security module (HSM) device for higher assurance and simplified management. Oracle uses the industry standard PKCS#11 interface to communicate with numerous HSM and external key management systems, including those provided by RSA, Thales, and Safenet. TDE supports key rotation by providing commands to change either the master encryption key or the data encryption key. Data encrypted with TDE will remain encrypted on backup media.

Oracle Advanced Security provides strong cryptography, supporting AES (128, 192 and 256 bits) and 3DES (2 and 3 keys; 168 bits).

Oracle Advanced Security provides protection for all communication to and from the Oracle Database, preserving privacy and confidentiality of data by preventing data sniffing, data loss, and replay and person-in-the-middle attacks. It provides both native network encryption and SSL/TLS based encryption for enterprises with PKI infrastructure. The Oracle database can be

configured to reject connections from clients that do not encrypt data, or optionally allow unencrypted connections for deployment flexibility.

Oracle Advanced Security TDE has been certified with numerous applications, including Oracle E-Business Suite and Oracle PeopleSoft Applications. In addition, SAP has certified with Oracle Advanced Security TDE. In addition, *Oracle Secure Backup* encrypts backups sent directly to tape and provides centralized tape backup management.

Privileged User Accounts

How Massachusetts Law Applies

Mismanagement and misuse of privileged user accounts puts PII at great risk of internal data breach. Privileged user accounts can include system administration and/or DBA accounts. These accounts are the target of hackers because they know these accounts have broad access to sensitive data. DBA accounts present high security risk because of their ability to configure systems, create users, modify and create databases and grant privileges.

While Massachusetts 201 CRM 17.00 does not explicitly call out control of privileged user accounts, it does call for restricting access based on job duties. In nearly all situations the system administrator and/or DBA does not require access to sensitive application data. Misuse of privileged user accounts puts an enterprise at severe risk of unauthorized use of PII and violation of the law. A review of some of the law's key provisions clearly demonstrate how organizations that fail to exert strong control over these accounts can expect to be held accountable by the attorney general. The law calls upon companies to:

- Implement access control measures that restrict access to records and files containing PII to those who need it to perform their duties. This is an important security tenet in general, which we'll address in subsequent discussion, but most critical—and, ironically, often most poorly implemented—for privileged accounts.
- Identify and assess reasonably foreseeable internal risks to records containing PII. Privileged users with too much authorization represent a high internal risk.
- Ensure employee compliance with policies and procedures. For example, privilege is often extended without following proper request and approval workflow.
- Monitor the security program to make sure it is operating in a manner to prevent unauthorized access to or unauthorized use of PII. Privileged user accounts should, in general, not have access to PII at all, but continuous monitoring is the only way to assure this.
- Monitoring of systems for unauthorized use or access to PII

- Assign unique identifications to each person with computer access. Privileged user accounts are often shared, so unauthorized persons can act injudiciously or maliciously without any accountability.

Hard to Control

Privileged user access control and authorization, and separation of duties are difficult to manage and maintain because of poorly defined roles and duties and privilege “drift,” as admins share user IDs and privileges are assigned in violation of policy or outside required workflow processes.

It’s easier to grant too much privilege than risk impeding operations by granting too little. Privileged authorization is frequently granted under pressure, but is never revoked. Privileged accounts and their passwords tend to be shared among multiple individuals as an expedience. Because it is difficult to establish highly granular controls, organizations tend to follow the path of least resistance and grant too much

As a result of loss of control over privileged accounts, monitoring, tracking and auditing of the responsible individuals’ activity is at best problematic.

Organizations need to review privileged accounts, and remediate the associated security risks. Privileged user roles must be strictly defined: controlling what systems and data they can access and what operations they are permitted to perform.

The challenges of managed privileged accounts is to give high-level users the ability to perform their jobs without access any access to, much less the ability modify or delete, PII. Enterprises must enforce separation duties, establishing appropriate user roles and — this is the hard part— provisioning and maintaining them under real world business conditions. Monitoring privileged user activity and generating audit trails for compliance and forensics is extremely difficult.

In short, managing privileged user accounts is essential for data security and compliance; getting it done using manual controls and reporting procedures is difficult, at best.

Oracle Manages Privileged Accounts

Oracle Database Vault enables organizations to enforce strong operational controls inside the Oracle database, providing additional protection for critical assets such as cardholder data from unnecessary risk and exposure. *Oracle Database Vault* provides powerful, yet flexible and easy-to-manage mechanisms to prevent privileged user access to sensitive application data, unauthorized changes to application structures and enforce separation of duty.

Oracle Database Vault enforces an internal firewall within the Oracle database using the concept of “realms”. Realms block all-encompassing DBA like privileges from being used for ad-hoc

access to application data while still enabling day to day database administration activities. Command rules enable multi-factor authorization controls prevent unauthorized changes to application structures and restrict access to databases to a specific subnet or application server, creating a trusted path for data access. Built-in factors such as IP address, time of day and authentication method can be used in a flexible and adaptable manner to enforce access control to meet compliance and business requirements.

Separation of duties is implemented in three baseline roles defined by responsibilities within the database: Account management, security administration and database administration. Each of these roles can be customized to meet specific business requirements.

Oracle Database Vault has been certified with numerous applications, including Oracle E-Business Suite, Oracle PeopleSoft Applications, Oracle JD Edwards Enterprise One, Oracle Siebel CRM and Oracle Retail. In addition, SAP has certified with Oracle Database Vault.

Oracle Database Firewall is Oracle's newest product addition and acts as the first line of defense for databases, helping prevent internal and external attacks from reaching the database. Highly accurate SQL grammar-based technology monitors and blocks unauthorized SQL traffic on the network before it reaches the database. Oracle Database Firewall is easy to deploy and requires no changes to existing applications. Oracle Database Firewall creates a defensive perimeter that monitors and enforces normal application behavior, helping prevent SQL injection, application bypass, and other malicious activity from reaching the database.

Oracle Database Firewall supports white list, black list, and exception list based policies. A white list is simply the set of approved SQL statements that the firewall expects to see. These can be learned over time or imported. A black list includes SQL statements that are not permitted to be sent to the database. Exception list based policies provide additional deployment flexibility that can be used to override the white list or black list policies. Policies can be enforced based upon attributes including SQL category, time of day, application, user, and IP address. Oracle Database Firewall can log and alert, block or substitute the incoming SQL statement with a harmless SQL statement. This flexibility, combined with advanced SQL grammar analysis, provides organizations graceful application handling of unauthorized requests.

Oracle Audit Vault securely consolidates audit data generated by Oracle and non-Oracle databases from across the enterprise into a secure central repository and provides dozens of audit and compliance related assessment reports covering privileged users, account management, roles and privileges, object management and system management. *Oracle Audit Vault* provides built-in alerting for suspicious activity as well as attestation for reports and email notification, requiring that designated individuals review reports. *Oracle Audit Vault* also provides integration with ticketing systems such as BMC Remedy. Oracle databases audit settings can be centrally managed using the *Oracle Audit Vault* console.

Access Control's Vital Role

201 CRM 17.00 Access, Authorization and Authentication

Centralized and highly automated identity management, incorporating granular, role-based access control, authorization and authentication provides not only essential security but enables the smooth flow of business operations.

Controlling user and application access is critical to protecting PII for compliance with Massachusetts 201 CRM 17.00. Identity management is a dynamic process, in which users, applications, data, and private and public networks are in constant flux, with access and authorization requests, new business initiatives and turnover of employees, contractors and partners.

The Massachusetts data protection law reflects the importance of identity management and lays out clear directives for access control, proper authorization and authentication. To recapitulate, it mandates:

- Secure user authentication protocols for controlling user IDs and other identifiers; secure assignment and selection of passwords and stronger authentication technologies, and provisioning policies and practices that assures that only active users have access to applications and PII.
- Secure access control measures that restrict access to PII based on business need. By implication this supports the case for granular role-based access control.
- Unique identifications plus passwords for each person with computer access.
- Regular monitoring to prevent unauthorized access to or unauthorized use of personal information

Access Control Challenges

These requirements seem straightforward and relatively simple at first glance, but the truth is that an enterprise-caliber identity management program that meets both the letter of the law and the clear intent behind it is difficult to implement, manage and maintain. These problems are generally the result of trying to enforce good policies with inefficient manual processes. The result is that organizations are unable to sustain compliance efforts on a continuous basis and inefficiently spend, manpower and money trying to manage almost unmanageable tasks, and gathering and analyzing data to verify controls and detect and remediate problems.

Let's examine why identity management programs often falter, as organizations struggle to manage and enforce consistent policy across a complex, distributed enterprise.

Access control, authorization and authentication is generally handled on a per application basis, rather than centrally managed. This creates uneven policy enforcement, heavy management overhead and slow, inefficient response to changing business requirements. It's difficult to apply appropriate authentication controls consistently across users, groups, applications and data access, in the absence of centralized, policy-based management.

Granular role-based access control is efficient and the most precise approach to access and authorization. But, it requires an enormous commitment of time and resources, in part because information about users, responsibilities and lines of reporting are typically in silos throughout the organization.

The identity management process is generally error prone for a variety of reasons. Role-based controls are difficult to define and manage without automated systems, so individuals are typically granted excessive privileges, based on coarse individual and/or group assignments, to assure that the individual has what he needs to perform his job.

Provisioning and de-provisioning users and user authorizations is slow and impedes the business. Spreadsheet-based administration can effectively enforce policy, but can become a bottleneck because of slow response by busy administrators and approvals by managers.

In addition ghost accounts persist after employees are terminated or long after a temporary need is past, giving unauthorized—and perhaps malicious—former employees access to sensitive data, such as PII.

Monitoring user activity is difficult. Since access control is managed separately for each application or system, monitoring and alerting is fragmented at best, or limited to spot checks.

Auditing is also piecemeal and inefficient, requiring manual data-gathering, analysis and reporting. It is almost impossible to correlate access information across disparate systems and applications.

A Program That Works

A successful identity management program effectively links all access to information, applications and systems to individual users and provides active, real-time monitoring to validate policy and detect errors. The enterprise also requires the reporting and audit trails that verify that controls are in place and effective—critical for demonstrating corporate diligence in the event of violation investigation and any emergent audit requirements, as well as internal compliance policies. A robust identity management program comprises:

- Centrally managed access control separated from individual applications so that access control can be maintained efficiently, according to policy, across the enterprise.
- Well-defined, granular role-based access control. Roles are created for particular job functions and the necessary permissions defined for each role. Roles can then be assigned to individuals, making it easy to add or change responsibilities.

- Timely and accurate provisioning and de-provisioning of employees, contractors and authorization privileges based on a well-defined evaluation and approval workflow.
- Real-time monitoring and alerting, comprehensive and timely auditing, and strong reporting.

To effectively create and maintain an identity management program that incorporates these capabilities, organizations should look to robust, well-integrated automated tools that provide centralized, granular authorization and access control, an efficient provisioning workflow, real-time monitoring, centralized audit logs and flexible, thorough reporting.

Oracle Identity Management

The Oracle suite of identity management products provides fully integrated centralized managed and automated access control, authorization and authentication; granular role-based access control and provisioning capabilities to effectively meet and exceed the Massachusetts law to protect PII, and all other regulatory and business requirements.

Oracle Access Manager secures access control through centralized authorization, authentication and audit, enabling single sign-on capabilities transparent to the user. By separating authorization from the application, companies can manage and monitor access privileges on an enterprise-wide basis, according to business requirements, based on policies and customizable rules.

The access system provides centralized policy-based authorization services, allowing admins to define policies that restrict access to specific resources by user, role, group membership (static, nested or dynamic), time of the day, day of the week and IP address.

Access Manager supports PCI authentication requirements, supporting X.509 certificates, smart cards, two-factor tokens and forms-based authentication. It allows organizations to establish hierarchies of authentication, so that a user might require only password authentication for general login to standard applications and information sources, but strong authentication, such as tokens, for more sensitive access.

Oracle Identity Manager is a robust provisioning and de-provisioning product that enables organizations to provision users quickly and easily based on business requirements, enhancing security and meeting 201 CRM 17.00 access control requirements, such as the mandate to restrict access to active users and accounts. *Identity Manager* is most effective when used in conjunction with *Oracle Identity Analytics*, which provides fine-grained role-based access control, allowing companies to precisely define and assign roles according to need, fulfilling the stricture to assign access and authorization based on the principle of least privilege and job classification and function.

Oracle's identity management products provide powerful monitoring, auditing and reporting capabilities to effectively provide assurance that controls are effective in accordance with

corporate policy, for internal compliance as well as defense in case of alleged violations. *Oracle Access Manager* sets and enforces policy-based authentication and monitors user access activity. *Identity Manager* detects rogue accounts and changes to user access privileges.

Access Manager's auditing services provide detailed and flexible logging, of monitored events, such as authentication success or failure as audit logs can be written either to a flat file or to a database and exported to any third- party reporting tool to produce comprehensive auditing reports.

Fraud Control

The risk of theft and fraud linked to misuse of PII grows as it flows between businesses, their customers and partner companies.

Oracle Adaptive Access Manager secures this growing environment, making it safer for enterprises to safely use PII. It provides real-time and context aware risk assessment, multi-factor authentication and authentication process hardening for Web applications. *Oracle Adaptive Access Manager* secures the free flow of information.

Conclusion

Massachusetts 201 CRM 17.00 sends the message loud and clear: The regulatory environment around data protection in general and personally identifiable information in particular continues to grow more demanding and more complex. The ascendance of the states' role in defining and enforcing data protection on behalf of their citizens presents the specter of a labyrinth of requirements.

Enterprises best response is a comprehensive data protection program, based on recognized security control frameworks, sound policies and risk assessments based on business needs. This type of program can only be realized through automated, integrated data security and identity management tools that create the necessary efficiencies for good security and smooth business operations.



Massachusetts Data Security Law Signals
New Challenges in Personal Information

Protection
August 2010
Author: Oracle

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com



| Oracle is committed to developing practices and products that help protect the environment

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

0109

