White Paper

BEST PRACTICES FOR CLOUD INFORMATION PROTECTION IN FINANCIAL SERVICES

How 5 Banks Complied with 10 Laws in 20 Countries with 1 Solution

CipherCloud®
Trust in the Cloud™

333 W. San Carlos Street
San Jose, CA 95110

Summary

◊ Cloud adoption continues to accelerate in the financial services industry as many companies realize the benefits of reducing their infrastructure, lowering costs, and becoming more agile.

◊ At the same time, there are increased concerns about the security and compliance of sensitive data that is stored in the cloud. A wide range of financial and privacy laws make organization directly responsible for protecting regulated information, but when this data is stored in the cloud they have less direct control over leaks, theft or forced legal disclosure.

◊ This paper gives an overview of major financial, privacy and data disclosure laws that govern customer data around the world, and potential penalties for inadvertent disclosure. In many cases, a single organization can be subject to overlapping or even conflicting laws in multiple countries.

◊ The biggest drivers for most organizations are the mandatory breach notification requirements of most compliance laws. While there can also be stiff fines and personal legal liability for business executives, the greatest concern is that even a minor leak can result in public disclosure, inevitable press, and massive potential damage to a company's brand and reputation.

◊ Also discussed are an increasing number of "Safe Harbor" exemptions to these breach notification laws, if an organization can demonstrate that data has been adequately protected through encryption, and no third-party has access to the encryption keys.

◊ To illustrate how these issues can be addressed, five major financial services organizations are profiled with details about how they deployed a solution to encrypt or tokenize data before it goes to the cloud, while maintaining exclusive control over encryption keys. This approach provides effective control over sensitive information regardless of where it's stored, making it safe to realize the business benefits of moving to the cloud.

Case Studies

Contents

Accelerated Cloud Adoption in Financial Services

In today's world, financial service businesses rely on communication technology and the rapid, but secure, sharing of information.

The very nature of financial systems requires that information about the availability of funds be discoverable, and accurately tracked. At the same time, the important factors of customer privacy, security and protection have resulted in a multitude of government regulations and oversight over financial services institutions.

Sharing, storing and distributing information using the cloud is a natural fit for companies that already use the Internet for vital financial communications. But like many new areas of technology, advances in sharing information are then followed by the need to secure it from misuse. This is especially true in the financial services industry where the loss or misuse of data can translate to financial losses, legal violations and outright theft of funds. Additionally, compliance with legal regulations for protecting sensitive data can be a significant challenge when that data may be created in one country, but stored in another that has different, overlapping, or conflicting laws.

It is, however, impossible for financial services firms to ignore or effectively restrict the adoption of cloud services. Utilizing the cloud has presented a significant reduction and consolidation in IT infrastructure, resulting in smaller budgets, more outsourcing, and an increase in value-added services for customers. There are dramatic potential business benefits and costs savings to be seen by deploying solutions in the cloud instead of on-premise, and many of these initiatives are driven by business units, rather than IT – often bypassing established deployment and security practices, according to the Forrester Research report: "Tracking The Renegade Technology Buyer."[(1)]

While it's no longer viable to "just say no" to the cloud, there are legitimate public concerns regarding security, privacy and financial transparency that are translating into more regulations with stricter penalties. What financial services organizations need are new models to assess risk with the cloud, and address compliance requirements, as well as new technology that allows them to proactively protect sensitive information before it goes to the cloud.

What Are the Biggest risks?

Criminal data theft in the financial services sector is an obvious and well-known threat, which is present with any type of communications or transfer medium, including the cloud.

Of perhaps equal concern to financial service institutions is the potential damage created by failure to comply with regulations, both domestically and internationally.

As business becomes increasingly global, financial services organizations can be subject to overlapping or even conflicting laws in multiple countries. For example, forced data disclosure laws in some countries might violate privacy laws of another country if the data crosses national boundaries – almost inevitable with the cloud.

The penalties for data breaches are continually increasing with stiff fines and legal liability for business executive. However, these fines are infrequently enforced and often not enough incentive to drive behavioral changes within large organizations.

The biggest concerns for most organizations are the Breach Notification requirements of most data privacy laws. Major or minor leaks can result in public disclosure, inevitable press, and massive potential damage to a company's brand and reputation.

This system of public breach notifications began with landmark privacy law in California enacted in 2002. State Bill 1386 requires any company that has lost or allowed access to unencrypted personal information to disclose the breach. Similar privacy laws with breach notification requirements now exist in 46 U.S. States and over 50 countries. Companies risk enormous hits to their brands and reputations if they are listed in a major notification. Many sites track these and news organizations are hungry to highlight mistakes by the latest big name company.

Case Study 1: Top 10 Global Bank

Based in the U.S. with over 200,000 employees serving business and consumer customers.

Challenges

- Building a consumer self-service loan portal to process a backlog of millions of mortgage loans to comply with Dodd-Frank consumer protection act and avoid millions of dollars in fines per day.
- Reducing costs and time-to-market by leveraging an existing and extensible cloud-based system – the Salesforce platform.
- Assuring compliance with financial and privacy regulations by guaranteeing that no one outside the bank can access protected information in the cloud.

Requirements

- Strong encryption for consumer identities and uploaded tax and income statements.
- Seamless integration with Salesforce, maintaining functionality, searching, indexing and ease-of-use of the platform.
- Integration with third-party products and backend legacy systems.

Solution

- CipherCloud for Salesforce was deployed in a clustered high availability configuration with hot disaster recovery.
- The system was integrated with real-time web services, customer VisualForce pages with Apex/SSP SAML assertions.
- Backend integration with IBM AS 400 iSeries with Informatica.

Results

- Ability to apply strong AES encryption on a field-by-field basis while assuring exclusive control over the encryption keys.
- Over 95% adoption rate with over 100 thousand customers, 1.5 million loans, encrypting over 2,500 files per hour.

Safe Harbor Exemptions

Increasingly, however, these regulations, take into account the use of encryption when the data loss occurs. In numerous cases, these laws recognize that if your data is adequately encrypted or "rendered unintelligible" then there are Safe Harbor exemptions from notification, and legal liability. While most regulations (other than PCI) don't specifically require encryption, they also recommend that encryption can be part of the solution, and eliminate the biggest risks of breach notifications. The table below outlines which major compliance regulations require mandatory breach notification and have exemptions if data is adequately encrypted:

Country/ Region	Regulation	Data Type	Mandatory Breach Notification	Safe Harbor Exemptions to Notification	Recommendations on Encryption
Worldwide	PCI DSS	Credit Card	Yes	Yes	Encryption or tokenization referred to as a "critical component"
U.S.	GLBA	Corporate Financial	Yes	Yes	Safe harbor only applies "if encryption has been applied adequately"
Europe	EU Directive 1995/46/EC	Personal Information	Proposed	Proposed	New draft regulation proposes notification safe harbor exemption if data was adequately encrypted.
Europe	EU Directive 2009/136/EC "EU Cookie Law"	Personal Information	Yes	Yes	Safe harbor exemption if data was adequately encrypted.
U.K.	ICO Privacy Amendment	Personal Information	Yes	Yes	Breach notification not required if there are "measures in place which would render the data unintelligible."
Australia	ICO Privacy Amendment	Personal Information	Yes	Not Specified	Does not specify encryption but requires organizations to "take adequate measures to prevent the unlawful disclosure" of protected information.
U.S. States	California SB 1386 (and similar laws in 46 states)	Personal Information	Yes	Generally Yes	Most state laws have similar definitions on: • *Personal Information:* "data elements that are not encrypted" • *Breach:* "unauthorized access to unencrypted data" • *Encrypted:* "use of an algorithmic process to transform data into a form which is rendered unreadable or unusable without use of a confidential key"

Overview of Financial Industry Data Regulations

The actual requirements of regulations affecting financial services organizations use of the cloud vary, however, a common misconception is that regulations will require companies to adopt a specific technology to be compliant.

In most cases, legal regulations require companies to protect personal and financial data, and use terms like "reasonable" and "adequate security," to define the steps that must be taken to do so. Aside from PCI regulations, the requirement to encrypt data may not be legally necessary, but it is highly recommended. The research firm Gartner notes in its report "Is Encryption of Centrally Stored Data Mandatory?"[2] that encryption requirements are "inconsistent" and the lack of these may "continue to add complexity and cost for enterprises." In an additional Gartner report, "Tackle Six Security Issues Before Encrypting Data in the Cloud,"[3] it is recommended that institutions using the cloud for communication and data storage "Use cloud encryption to protect sensitive data for three scenarios: 1) data residency issues, 2) to provide exemption from data breach notification requirements and 3) to "digitally shred" sensitive cloud data at its end of life by deleting the encryption keys."

Several of the major regulations listed below have a significant impact on financial services industry organizations seeking to remain compliant with domestic and international regulations.

Case Study 2: Top 5 Canadian Bank

150 year-old bank with over 40,000 employees, providing retail, business and wholesale banking services.

Challenges

- Building a banking CRM system for sharing M&A and IPO data with partner in many countries globally.
- Leveraging the cloud-based Salesforce platform (including Chatter and Force.com) to reduce development time and operational costs.
- Complying with Canadian privacy laws (PIPEDA) while using U.S.-based cloud services, potentially risking data disclosures through the U.S. Patriot Act.

Requirements

- Encrypting any personally identifiable information (PII) and financial data to assure compliance.
- Protecting both structured data (fields in Salesforce) and unstructured data (Chatter feeds) with strong encryption for consumer identities and uploaded tax and income statements.
- Preserving usability of the application and access by mobile users.

Solution

- CipherCloud for Salesforce and Chatter was deployed in a high-availability, load-balanced cluster.
- Integration with Cognos, Kerberos along with custom VisualForce pages/Apex.

Results

- Ability to apply strong AES encryption on structured and unstructured data.
- Enabled their cloud initiative by meeting strict Canadian and international compliance requirements.
- Dramatically reduced development costs and time-to-market by using a cloud platform versus conventional on-premise solutions.

Financial Industry Data Regulations

Payment Card Industry Data Security Standard (PCI DSS)

This worldwide information security standard was created to protect credit and customer account data from unauthorized access and misuse. To meet the PCI security specification for credit card storage, the following objectives must be met:

- Protect the credit card number, expiration date, service code and card holder's name from logical or physical access;
- Use access controls to provide separation of duties between administrators and users who access credit card numbers;
- Securely store encryption keys, protecting them from exposure, unwanted replacement or misuse, and establish procedures to provide 'dual control' over key management;
- Log access and administration of key management and PAN data storage systems;
- Document your process and protection measures.

While PCI DSS serves more as general guidance than an operational checklist, it requires organizations to render stored Primary Account Numbers (PAN), i.e. credit card numbers, unreadable. You can hash, truncate, tokenize, or employ other forms of irreversible obfuscation, but it's likely that you will need to keep the original data and occasionally access it for payment remediation or auto-payment. Thus encryption or tokenization is usually the answer, and even when you use tokenization you still need to encrypt the original PAN data in the secure token database.

PCI DSS addresses cloud computing as an instance of "shared hosting," and specifies that providers must segregate cardholder data environments, enforce access control, and support logging, audit trails, and forensic investigations. To comply with PCI DSS requirements with cloud applications financial services industry enterprises must employ granular encryption controls, key management, and auditing controls.

Financial services industry enterprises must employ granular encryption controls, key management, and auditing controls.

Financial Industry Data Regulations

GLBA (501(b) of United States Gramm-Leach-Bliley Act)

Requires financial institutions to establish appropriate standards for protecting the security and confidentiality of their customers' non-public personal information.

The standards' objectives are to:

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records, and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

The GLBA guidelines require institutions to consider whether encryption of electronic customer information while in transit or in storage is appropriate. The Federal Financial Institutions Examination Council (FFIEC) states the following: "Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit." Therefore, under GLBA, a financial institution that does not deploy encryption may be called upon by the FFIEC to prove that it considered deploying encryption and justify why it decided against it.

In addition to the GLBA, the United States government has also instituted several related laws, including Sarbanes-Oxley and Dodd-Frank, to monitor financial services industry institutions against misuse of information and data loss.

Case Study 3: Leading Wall Street Investment Company

Market-leading 75 year-old firm, with over 60,000 employees providing investment banking, brokerage and commodities services.

Challenges

- Moving traditional on-premise application development to more flexible and powerful Force.com cloud-based platform.
- Migrating an initial 300 applications out a portfolio of over 4,000 applications on custom platforms.
- Finding a flexible and robust security platform for a wide range of existing and future cloud-based applications.

Requirements

- Assuring security and compliance for custom applications built on a public-cloud platform.
- Ability to encrypt or tokenize large amounts of sensitive data on-the-fly with minimal latency.
- Deploying a single platform with a range of security options to protect an unlimited number of disparate cloud applications.

Solution

- CipherCloud for Force.com platform to be implemented with a wide array of custom-developed financial and customer-facing applications.
- High-performance AES encryption and tokenization of sensitive data for large-scale deployments.

Results

- After rigorous testing and validation, the CipherCloud platform received approval from multiple design and IT groups within the bank including Enterprise Architecture, Information Security, Cryptography Services, and Network Operations.

Financial Industry Data Regulations

U.S. State Privacy Laws

To date, 46 U.S. states have enacted data privacy laws, often modeled after California's SB 1386. Most of these laws are designed for protect misuse or disclosure of personal information including names, social security numbers, driver's license numbers, account numbers, credit or debit card numbers, as well as access codes or passwords that would permit access to an individual's financial account, medical or health insurance information.

Most state privacy laws specifically exempt encrypted data if it has been "transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key."(2)

Details on all U.S. state breach notification laws can be found on the National Conference of State Legislatures website: www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

Case Study 4: Leading Provider of Financial Loyalty Programs

Supporting over 5,300 financial partners globally with over 65 million members.

Challenges

- Aggressively moving IT functions including email systems to the cloud to streamline global operations.
- Handling credit card, personal information and financial data for millions of members.
- Assuring compliance with PCI-DSS as well as dozens of regional financial and privacy laws.

Requirements

- Moving internal Microsoft Exchange email servers to the cloud via Office 365.
- Supporting over 5,000 users in America, Europe, and Asia with cloud-based email.
- Providing access across multiple browsers, Outlook clients, and mobile devices.

Solution

- Deployed CipherCloud for Office 365 on virtual servers hosted on Amazon Web Services (AWS) with load balancing and active-active clustering.

- AES encryption of all email at rest in Microsoft cloud servers, including In Boxes, Sent Items, Archives, and Calendars.
- Integration with third-party MAPI and ActiveSync of mobile devices.

Results

- Dramatically reduced email infrastructure and administrative costs.
- Freed critical IT resources to focus on value-added core business functions.
- Met compliance requirements while assuring higher levels of data protection than previously available in-house.

Financial Industry Data Regulations

European Union Data Privacy Directives

European Union has enacted both the Data Protection Directive of 1995 (46/EC) as well as the Internet Privacy Law of 2002 (58/EC). These were developed create standards among EU member states, as diverging laws were impeding the free flow of data within the EU. These Directives reflect broad personal privacy laws throughout Europe, and cover the electronic processing and storage of personal information.

Requirements include:

- Notice—that personal data is being collected
- Purpose—data should only be used for stated purposes
- Consent—data should not be disclosed without the subject's consent;
- Security—collected data should be kept secure from any potential abuses;
- Disclosure—subjects should be informed as to who is collecting their data;
- Access—subjects should be allowed to access their data and make corrections to any inaccurate data; and
- Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles.

More than 28 EU countries have established privacy laws that reflect the EU Directives, although there are regional differences in how these are interpreted.

The UK Data Protection Act

In the UK, the Information Commissioner's Office (ICO), which has the ability to levy half a million pounds in fines for companies that contravene the Data Protection Act, has recently turned its attention to the cloud.

In November 2012, it published guidance outlining the responsibilities for companies storing their customers' data in cloud environments.

The guidelines assign responsibility for data security unequivocally to the company that owns the data, rather than the company taking care of it. Any organization with customer data processed by a cloud service provider that has a data breach may want to blame the third party, but the ICO has made it clear that the owner of the data is responsible.

Financial Industry Data Regulations

Australia Privacy Amendment

Australia has actually had a Privacy Act in place since 1988, but has now taken steps to bring its law up to date with The Privacy Amendment Act of 2012 (Enhancing Privacy Protection Reform Act).

The updated Privacy Act is explicit that enterprises that hold Australian customer data are responsible for protecting that data, regardless of where it's located, or whether breaches are caused by cloud providers.

The law states that "reasonable" steps must be taken to protect personal information and that organizations must demonstrate "prudent" practices for information protection to avoid investigation and penalties.

The Privacy Amendment specifically discusses cross-border disclosure of personal information. If overseas cloud providers are not subject to Australian law and there is a breach, then the Australian entity that owns the data is financially and criminally liable.

According to an Australian Privacy Commissioner, "if an offshore cloud compromises your data we'll sue you, not them".

Case Study 5: Leading Australian Bank

Top 40 global bank with over 40,000 employees, providing banking, fund management and insurance services.

Challenges

- Traders requiring a global collaboration system while assuring that sensitive information doesn't violate regional data residency laws.
- Leveraging the Salesforce for Chatter application to provide easy web and mobile access for sharing transaction data.
- Complying with Australian privacy laws as well as explicit data residency laws in Luxembourg.

Requirements

- Support for over 32,000 users in multiple countries.
- Encrypting sensitive information in unstructured Chatter posts to assure compliance.
- Tokenization of specific types of data to assure compliance with data residency laws in Luxembourg.
- Preserving usability, search and index functions of the Chatter platform.
- Seamless access via multiple types of web browsers and mobile devices.

Solution

- CipherCloud for Chatter was deployed in a high-availability architecture.
- High-performance AES encryption as well as tokenization with local storage for data residency compliance.

Results

- Assures compliance with Australian and international data privacy and data residency laws.
- Enabled the use of a cloud-based platform by assuring that sensitive information can only be accessed by authorized employees and partners.

Financial Industry Data Regulations

Data disclosure laws – U.S. Patriot and similar laws in other countries

The U.S. Patriot Act is often cited as a cause for concern, especially organizations outside the U.S., when considering whether to user cloud services. In fact, almost all countries have rules that allow law enforcement agencies to access customer data directly though a service provider, often without notifying the customer.

For many financial services organization, especially outside the U.S., these forced disclosures can potentially violate national data privacy laws. This is often cited as a concern or inhibitor for many corporate cloud initiatives – the organization is legally required to protect personal information, but can't be certain that it won't be accessed by law enforcement in other countries.

> Almost all countries have rules that allow law enforcement agencies to access customer data directly.

Most organizations regularly deal with legal subpoenas to turn over data, but they want to manage and accurately comply with specific requests themselves. The risk of having a cloud provider turn over potentially large amounts of data, causes heartburn for most corporate legal departments.

Best Practices for Cloud Information Protection

In order to leverage the advantages of the cloud, while fully protecting sensitive information, financial services organizations need to take a holistic view towards data security and compliance. The following steps are recommended as part of an ongoing process to identify, secure and monitor information for legal compliance:

Discover

Before you can protect sensitive corporate information in the cloud you first need a detailed understanding of:

- Who should have access and who should not;
- What content is sensitive, proprietary, or regulated and how can it be identified;
- Where this data will reside in the cloud and what range regional privacy, disclosure and other laws might apply.

Protect

Finding effective and practical tools to protect the right information assuring that:

- No unauthorized outsiders can ever access, leak or disclose protected data because your organization maintains the exclusive access to decryption keys;
- You have granular control to apply the appropriate level of security to specific types of data including encryption, tokenization, data loss prevention, malware protection;
- The solution provides extensive visibility and reporting of information going to and from the cloud assuring that you can monitor and audit cloud activity and demonstrate compliance with regulations.

Enable

No security solution will be effective if it breaks the application or makes it impractical to use. In order to safely leverage the advantages of the cloud you need solutions that:

- Preserve the formats, fields, and function of the data when it is secured for both structured and unstructured data;
- Support tools critical to users such as searching, sorting, indexing and reporting on data while it is secured in the cloud;
- Provide a single platform that supports any type of cloud application and integrates with third-party enterprise tools, such as SSO, DLP, key management, and audit log reporting.

Monitor

On-going monitoring of information going into the cloud requires detailed visibility, application awareness, and understanding of the context of business information. Solutions need to:

- Enable granular reporting and visibility into cloud application usage, with context on user roles, content, and accessibility to specific types of data
- Provide granular, field-by-field information on the types of information that are being protected and by what security methods.
- Assure monitoring of DLP policies, violations, and actions taken to address anomalies.
- Correlate between multiple cloud applications to provide consistent controls enterprise-wide.

Conclusions

Adoption of the cloud is passing a tipping point and is increasingly a fact of life for many financial services organizations.

But this change in technology does not absolve organizations from their legal responsibilities to protect their customer's data. In fact, the growth of the cloud has been met with an equal growth in privacy laws and data residency restrictions. Business units and IT need to collaborate in finding new security models to leverage the cloud while assuring protection for sensitive information.

By leveraging new cloud security technology, organizations can resolve these conflicting interests – retaining control over their sensitive information, while enabling the business to realize the many benefits of the cloud. By deploying systems that encrypt sensitive data at the gateway, while keeping all encryption keys within the enterprise, organizations can safely extend their virtual security perimeter to include global, distributed cloud services, while still maintaining privacy, security, and compliance.

As illustrated by the customer examples in this paper, CipherCloud provides comprehensive cloud information protection for many of the world's largest and most security-conscious financial services organizations.

(1) Forrester Research: Tracking The Renegade Technology Buyer, John C. McCarthy, May 6, 2013
(2) Gartner: Is Encryption of Centrally Stored Data Mandatory?, Brian Lowans, Jeffrey Wheatman, Aug 31 2012
(3) Gartner: Tackle Six Security Issues Before Encrypting Data in the Cloud, Brian Lowans, Neil MacDonald, March 9 2012

CipherCloud is the leader in cloud information protection enabling organizations to securely adopt cloud applications by overcoming data privacy, residency, security, and regulatory compliance risks.

Visit **www.ciphercloud.com**
for more information, online demos, or free trials.

Email **sales@ciphercloud.com** or call +1.408.520.4937

Corporate headquarters:
99 Almaden Blvd,
San Jose, CA
95113, USA