



BANKING SECURITY and COMPLIANCE

BANKING SECURITY AND COMPLIANCE

W H I T E P A P E R

Cashing In On Banking Security and Compliance

With awareness of data breaches at an all-time high, banking institutions are working hard to implement policies and solutions that protect sensitive financial information along with their reputations and industry competitiveness. In today's digital world, critical financial data—including social security numbers, bank account information, mortgage statements, payment card numbers, and other high-value, highly confidential information—is being sent back and forth between businesses and individuals at speeds faster than anyone ever thought possible. While this information exchange allows financial institutions such as banks to deliver higher levels of service and capitalise on emerging growth opportunities, it also leaves them vulnerable to security breaches and data leaks.

For financial organisations, data security is an operational and, at the same time, regulatory imperative. A bank that fails to protect a customer's financial records faces the threat of losing customers—whether they are individuals or businesses—along with a tarnished reputation, class-action lawsuits, and the loss of competitive advantage.

Financial institutions face the risk of data breaches every day. These breaches can occur when data is being transferred to customers, vendors, and other institutions; when it is being stored; and when it is being processed. Threats can include the theft of computer equipment, employee malfeasance, and sophisticated hacking and phishing attacks. Recent high-profile banking data breaches include:

- A compact disc containing personal information of more than 370,000 customers of HSBC was lost after being sent by courier. The bank was subsequently fined over £3 million by the Financial Services Authority (FSA).
- The UK branch of Zurich Insurance had to write to 51,000 of its customers to inform them of a data loss. The back-up tape was lost during a routine transfer within South Africa to a data storage centre in August 2008

EXCEEDING COMPLIANCE REGULATIONS

Ipswitch File Transfer solutions ensure the compliance and security of financial information with support for current industry regulations:

Gramm-Leach-Bliley Act (GLBA)

Protects consumers' personal financial information held by financial institutions.

Payment Card Industry Data Security Standard (PCI DSS)

Safeguards payment cardholder data and sensitive card authentication information.

Sarbanes-Oxley Act (SOX)
Protects public company financial information.

BASEL II

Ensures the soundness and stability of the international banking system using risk management strategies.

BANKING SECURITY AND COMPLIANCE

W H I T E P A P E R

- In 2007 the FSA imposed a £980,000 fine on the mortgage lender Nationwide Building Society after an employee laptop with data on millions of customers was stolen.

Effective information security practices are more important than ever in the challenging times currently facing the banking industry. In the finance and banking sector the Data Protection Act, presided over by the FSA, and the Gramm-Leach-Bliley Act (GLBA) govern the collection and disclosure of customers' personal financial information and requires that financial institutions design, implement, and maintain safeguards to protect this information. The acts contain important provisions requiring that customer data be protected not only by those institutions that collect it, but also by all financial institutions that receive information from other financial institutions. In other words, vendor management is a critical component of your compliance strategy. Proper risk-assessment requires that you be aware of your vendors' security and compliance status as well as your own.

Compliance with GLBA is mandatory and the regulation includes severe civil and criminal penalties for non-compliance, including fines of up to \$100,000 for each violation, personal fines, and the loss of deposit insurance, such as that provided by the Federal Deposit Insurance Corporation (FDIC) in America. In today's climate, no financial institution that deals with sensitive financial information can afford to ignore the very real challenge of ensuring data security, integrity, and privacy.

The Risks of Insecure Data Transfer

With the increasing popularity and ease of electronic storage and transfer, interest in the safety and integrity of this sensitive data is at an all-time high. Banks have traditionally relied on methods like tape backup, DVDs, network storage, FTP, email, and even instant messaging to move data between partners, branches, and customers. While these methods are convenient, they fail to deliver security, efficiency, or reliability—all of which are critically important to today's financial organisations.

Tapes, DVDs, and laptops can be stolen or lost, compromising the data they contain, particularly if the data is unencrypted. Standard FTP does not include strong authentication or encryption capabilities, which opens the door to the potential for hackers to access sensitive data. While email and instant messaging lack scalability and use server resources inefficiently, the larger problem with these methods involves their lack of encryption and data integrity. In addition, following the receipt of records, neither email nor IM have processes for workflow, data integrity verification

BANKING SECURITY AND COMPLIANCE

W H I T E P A P E R

to make sure the entire transmission arrived untouched and uncompromised, or the ability to enforce business rules to control access to those records.

A Better Way to Ensure Financial Confidentiality

To operate effectively, banks must replace ungoverned document transfer and storage methods with secure, reliable, and compliant information exchange processes that ensure data integrity. These processes help financial organisations move confidential data between locations in a secure, accurate, controlled, and documented manner that addresses the full range of current and evolving legislative and regulatory mandates.

A secure file transfer solution enables financial organisations to send data more securely with return receipts and extensive tracking and auditing capabilities to ensure compliance with BASEL II, GLBA, PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley Act) and regulations imposed by the FSA. Two common security protocols that help secure and increase the reliability of data transfer are Secure Sockets Layer (SSL) and Secure Shell (SSH). Both are specifically designed to encrypt file transfers as well as the associated administrative network traffic. SSL and SSH enhance the security and reliability of file transfer by using encryption to protect against unauthorised viewing and modification of high-risk data during transmission across open networks such as the Internet.

Data must also be protected when it is being processed, in transit, and in storage. Financial organisations should use the strongest commercially available cryptography for storing and transporting data: 256-bit AES SSL. Combining SSL and SSH security with OpenPGP provides an additional level of protection for data at rest. OpenPGP encrypts files in storage through the use of cryptographic key pairs that authenticate users and data. Receivers need to use the corresponding private key in order to decrypt the file.

Additional security measures include the use of FIPS 140-2 validated encryption libraries to secure files in transit, using 256-bit AES encryption and SHA-1 libraries to secure files in storage, and using the smallest possible buffers to secure files when processing them between transfer and storage encryption in order to prevent the exposure of large chunks of sensitive information in memory. To prevent even encrypted files from lingering on disk longer than absolutely necessary, files should be overwritten with cryptographic-quality random data upon deletion. The ideal level of data erasure is NIST 800-88 compliant and fulfils a critical PCI requirement.

BANKING SECURITY AND COMPLIANCE

W H I T E P A P E R

Making Secure and Managed File Transfer a Reality

An effective data transfer solution must be able to ensure end-to-end security, reliability, and auditability throughout the file transfer process, and provide management visibility over the process via integrated, application-level security, compliance reporting, auditing, workflow monitoring, and automation. Important features to look for in a data transfer solution include the ability to:

- Reduce the risk of providing access to financial data while complying with regulations such as BASEL II, GLBA, PCI DSS, SOX and those from FSA
- Simplify and automate file transfer processes to better understand, monitor, and respond to changing requirements without compromising customer confidentiality
- Protect file transfer communications through embedded security
- Provide robust data management, monitoring, and scheduling that includes tracking, auditing, and guaranteed delivery with non-repudiation

Four Critical Considerations

When evaluating technology solutions for data security, you should look at how four categories—confidentiality, integrity, availability, and auditing—contribute to compliance.

Confidentiality ensures that information can only be consumed by authorized individuals and only for approved uses. Confidentiality begins with authentication of login credentials and putting a strong password policy in place, with features like expiring accounts and password management. Access control includes support for requiring 256-bit AES SSL encryption and TLS 1.1 or higher on all connections. This level of access should be mandatory for all clients connecting into your network infrastructure. If the clients connecting to your file transfer platform can't connect at 256-bit SSL or SSH or higher, access should be denied in order to protect your company from a potential data breach.

Integrity means ensuring you have uncompromised delivery of all correct data with full SHA-512 support. Secure, encrypted data delivery is critical for ensuring business continuity. Secure hashing algorithms ensure that files have not been compromised during transport, and that the source and destination files are exact matches. A single change in a file or writing a file to a bad sector on a disk can corrupt a file and produce faulty workflow notifications and business

BANKING SECURITY AND COMPLIANCE

W H I T E P A P E R

process events. Non-repudiation takes data security to the highest level currently available by adding digital certificate management to secure delivery and data encryption.

Availability can be achieved through load balancing and clustering architectures that support automatic failover and centralised configuration data storage to minimise the chance of a data breach. This also helps protect against anti-hammering and distributed denial of service attacks. Availability can also be achieved by building checkpoint restart and robustness into the solution that can overcome hardware failures or interruptions in Internet connectivity.

Auditing provides comprehensive logging and log viewing with tamper evident security to guarantee the integrity of the log files. For technology, security, and other auditing purposes, all client/server interactions and administrative actions should be logged. A full MFT solution includes analysing capabilities, and features native and custom reporting and event driven notifications and workflow to ensure banks know what's happening on their networks, and that they'll be prepared to respond in the event of a compliance audit.

IPSWITCH FILE TRANSFER: SECURE, MANAGED, AND COMPLIANT SOLUTIONS

Ipswitch solutions deliver secure and managed end-to-end file transfer, enabling banks to meet GLBA, SOX, PCI DSS, and other compliance objectives and still have ready access to necessary financial information.

Safeguard financial information

Ipswitch file transfer solutions provide 256-bit AES encryption for transfers over SSL (FTPS, HTTP/S), SSH (SFTP, SCP2), and EDIINT (AS1, AS2 and AS3) protocols — the highest commercially available encryption technology — making them the most secure solutions for banks that require confidentiality when transferring financial data over the Internet.

Ipswitch solutions also leverage OpenPGP file encryption, up to SHA-512 integrity, to ensure uncompromised transfers and non-repudiation.

Exceed stringent regulatory requirements

Our secure, automated, and reliable solutions track data access and security enforcement policies to enable a level of GLBA, PCI DSS and SOX compliance unrivaled by other file transfer methods. With the ability to create multiple hosts,

BANKING SECURITY AND COMPLIANCE

W H I T E P A P E R

control user access down to the file level, and block attacking IP addresses in real time, administrators can help to ensure that confidential data is only accessible by those with explicit permissions.

Increase ease of use and control IT operational and training costs

Ipswitch solutions feature intuitive graphical user interfaces that are easy to configure and require no expensive training. Secure web-based interfaces let administrators control access, define rules, and ensure enforcement from one customisable dashboard. Silent installs and virtualization are also major cost-control mechanisms supported by Ipswitch solutions.

Improve customer satisfaction

The Ipswitch file transfer architecture scales to thousands of servers and clients — providing the server clustering and load balancing necessary to ensure the availability and performance of critical merchant applications, and ensuring quick, seamless, and secure customer transactions.

About Ipswitch, Inc.

Ipswitch File Transfer is a global technology provider that builds solutions to securely move your valuable data. We enable companies and people to better manage their data interactions when visibility, management and enforcement matter. Our managed file transfer solutions deliver the control necessary to enable governance and compliance for our more than 40 million global users – including the majority of Fortune 1000 enterprises and government agencies. These organizations trust Ipswitch File Transfer solutions to secure, manage, automate and streamline their critical and highly sensitive file transfers and data workflows. Learn more at <http://www.ipswitchFT.com> or to contact us at <http://www.ipswitchft.com/Company/Contact.aspx>, or on [LinkedIn](#) and [Twitter](#).