Voltage security

Secure Messaging for Financial Services

Conforming to GLBA Safeguards

Contents

All information in this document is subject to change without notice. This document is provided for informational purposes only and Voltage Security, Inc. makes no warranties, either express or implied, in this document.

Voltage SecureMail, SecureFile, SecureDisk and IBE Server are trademarks of Voltage Security, Inc. All other company and product names may be trademarks of their respective owners.

INTRODUCTION

The banking and financial systems of our nation and the world community are critical to our economies and well-being. U.S. Treasury Secretary John Snow told the U.S. Senate that, "The financial system is the lifeblood of our economy."[1] Another Treasury official expanded this point: significant disruptions in the financial system "would severely affect our economic growth and our standard of living."[2]

Financial institutions face particularly acute cyber-risks. They hold among the most sensitive personal information that their customers would share with anyone. Information in the possession of financial institutions, in the wrong hands, can permit attackers to steal the identity of customers, open fraudulent accounts, and make fraudulent purchases.

In several highly-publicized cases, thieves stole credit card databases from online merchants. In 2000, Creditcards.com, CD Universe, and Egghead.com[3] fell victim to database thieves. The thief in the Creditcards.com and CD Universe incidents even posted the stolen numbers on the web. In 1999, the government indicted the successor of a company called Interloc, Inc. for intercepting emails. The emails originated from the online bookseller Amazon.com and were intended for Interloc's book dealers. Interloc intercepted the emails for the purposes of data mining and analyzing the book market. Interloc provided Internet services to these dealers, and therefore had access to the emails coming to the dealers, enabling Interloc to intercept and store emails from Amazon.[4] While these cases do not involve financial institutions themselves, they suggest that financial institutions, with large amounts of financial information, are likely targets of attacks.

Security breaches involving financial institutions themselves confirm their vulnerability. Consider the following examples:

- Unauthorized access and control of cash management system led to a diversion of more than $10 million from Citibank into accounts under the control of thieves. Their exploit involved stolen passwords and identification numbers.[5]

- In two separate incidents, a Wells Fargo consultant and a Wells Fargo employee became victims of laptop thefts. In a November 2003 incident, a thief broke into the office of the

[1] Testimony of John Snow, Senate Appropriations Committee, Subcommittee on Transportation, Treasury and General Government (Apr. 20, 2004), *reprinted at* http://www.treas.gov/press/releases/js1444.htm.

[2] Brian Roseboro, Acting Under Secretary of the Treasury Domestic Finance, Department of Treasury, *quoted in* Financial Services Information Sharing and Analysis Center, "About the Financial Services ISAC" <http://www.fsiac.com/aboutus.cfm>.

[3] CNN.com, *Hacker steals huge credit card database* (Dec. 13, 2000) <http://www.cnn.com/2000/TECH/computing/12/13/credit.cards.com.hacked/index.html>; USA Today, Troy Wolverton, *FBI probes extortion case at CD store* (Jan. 10, 2000) <http://marketwatch-cnet.com.com/2100-1017_3-235418.html>; Lori Enos, *Credit Cards Safe Despite Hack, Egghead Says* (Jan. 8, 2001).<http://www.ecommercetimes.com/perl/story/6541.html>.

[4] U.S. Dept. of Justice, *Internet Service Provider Charged with Intercepting Customer Communications and Possessing Unauthorized Password Files* (Nov. 22, 1999) (press release), *reprinted at* http://www.usdoj.gov/criminal/cybercrime/alibris.htm.

[5] Statement of Michael A. Vatis, Director, National Infrastructure Protection Center, before the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee (Feb. 29, 2000), *reprinted at* http://www.house.gov/judiciary/vati0229.htm.

consultant and stole a laptop containing names, addresses, and social security numbers of thousands of customers.[6] In the second incident, a thief stole the rental car that the employee had been using at a gas station; the laptop containing sensitive financial information.[7]

- In a similar laptop theft incident involving Bank of Rhode Island, the Bank lost information concerning 43,000 customers, more than half of the Bank's customer base.[8]

The use of the Internet to do more kinds of transactions in recent years only increases the risk. Financial service providers are constantly rolling out new online services to expand new markets and reduce transactional costs. Examples include, besides online banking itself, online securities trading, loan and insurance applications, and bill payment services. With real-dollar transactions occurring over the Internet, the potential is greater for fraud, interception, and identity theft.

THE GRAMM-LEACH BLILEY ACT (GLBA) AND FINANCIAL SERVICES SECURITY

1. GLBA and Established Security Standards

In an effort to address growing national concerns about privacy, Congress enacted and President Clinton signed the Gramm-Leach-Bliley Financial Modernization Act (GLBA)[9] in 1999 Among the various things that it does, GLBA reflects Congress's policy that "each financial institution has an affirmative continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[10] This policy reflects the understanding that security is an important foundation to achieving privacy protection.

GLBA covers "financial institutions." That category is a broad one. In addition to the institutions that immediately come to mind – such as banks, savings associations, credit unions and the like – it also covers businesses that are "financial in nature," - such as insurance carriers, tax and financial advisors, money transmitters, and pay day lenders.[11] Many businesses may be surprised to discover that they fall under GLBA, even though they consider themselves very different from the typical example of financial institutions, banks.

[6] David Lazarus, *A simple theft nets Wells a world of woe; Break-in behind bar puts clients' data at risk*, S.F. CHRONICLE (Nov. 21, 2003).

[7] Identity Theft 911, LLC, *Wells Fargo Does it Again* (Apr. 16, 2004) <http://www.identitytheft911.com/education/articles/art20040416wells.htm>.

[8] Identity Theft 911, LLC, *Stolen Laptop May Contain Personal Info for Bank of Rhode Island Customers* (Dec. 22, 2003), *reprinted at* http://www.collectionsworld.com/cgi-bin/readstory.pl?story=20031222CCWI815.xml.

[9] Gramm-Leach-Bliley Act, Public Law No. 106-102, Statutes at Large, vol. 113, page 1338 (1999) [called "GLBA" in this white paper].

[10] Title 15 United States Code ("U.S.C.") Section 6801(a).

[11] The definition of "financial institution" in GLBA, 15 U.S.C. § 6809(3)(A) refers to a description in another law, 12 U.S.C. § 1843(k), which speaks of activities that are "financial in nature or incidental to a financial activity."

On November 16th, 2004, the Federal Trade Commission (FTC) announced that it was charging Nationwide Mortgage Group, Inc. and Sunbelt Lending Services, Inc. (a subsidiary of Cendant Mortgage Corporation) for violating the agency's Gramm-Leach-Bliley Act (GLBA) Safeguards Rule. According to the FTC news release, both companies failed to implement safeguards to protect its customers' sensitive financial information including: names, social security numbers, credit histories, bank account numbers, and income tax returns.

This action represents the first cases involving the Safeguards Rule. Jessica Rich, assistant director of consumer protection at the FTC, said, “The companies were part of a "nationwide sweep" of auto dealers and mortgage companies.” She said the FTC hoped the action sent the message that the Safeguards Rule applies not only to typical financial institutions but also to payday lenders, check cashers and tax preparers who handle sensitive personal information when conducting business.[12]

GLBA assigns the different categories of financial institutions to various federal agencies and state insurance authorities for oversight.[13] These agencies have the authority to enforce GLBA. Regarding information security, GLBA charges each of the agencies with establishing “appropriate” security standards for the financial institutions they regulate.[14] These standards must relate to “administrative, technical, and physical safeguards.”[15]

The agencies’ standards must, firstly, ensure “the security and confidentiality of customer records and information.”[16] Secondly, the standards must “protect against any anticipated threats or hazards to the security or integrity” of these records.[17] Finally, the standards must “protect against unauthorized access to or use” of the records that could cause customers to sustain “substantial harm or inconvenience.”[18]

In response to these instructions, the various agencies adopted regulations to implement security standards. A group of these agencies banded together to create a single set of guidelines for the businesses that they regulate: the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Interagency Guidelines).[19] Each of these agencies issued regulations requiring financial institutions under their oversight to follow the Interagency Guidelines.[20] The agencies issuing the Interagency Guidelines are members of

[12] Computerworld, Inc, “FTC Charges Firms over Web Breaches”, November 22, 2004.

[13] Examples include the Office of the Comptroller of the Currency (OCC) (for national banks), the Federal Reserve System (for Federal Reserve banks), Office of Thrift Supervision (OTS) (for savings associations), and the National Credit Union Administration (NCUA) (for credit unions). 15 U.S.C. § 6805(a). The FTC has general jurisdiction to cover any financial institutions that are not covered by one of the other agencies. 15 U.S.C. § 6805(a)(7).

[14] 15 U.S.C. § 6801(b).

[15] 15 U.S.C. § 6801(b).

[16] 15 U.S.C. § 6801(b)(1).

[17] 15 U.S.C. § 6801(b)(2).

[18] 15 U.S.C. § 6801(b)(3).

[19] Vol. 66 Federal Register (“Fed. Reg.”), page 8616 (Feb. 1, 2001). The agencies adopting the Guidelines are the OCC, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and OTS.

[20] More specifically, agencies adopting the Guidelines have either required compliance directly, or have required them indirectly by including them in the “safety and soundness” factors that the regulators consider. Title 12, Code of Federal Regulations (“C.F.R.”), Section 30.3(a) (OCC’s regulation); 12 C.F.R. § 308.302(a) (FDIC’s regulation). Regulators can seek to close a financial institution if

the Federal Financial Institutions Examination Council (FFIEC).[21] The versions of the Interagency Guidelines adopted by the various agencies are substantially similar, although not identical. Other agencies established their own regulations to establish GLBA security standards.[22] The States have adopted various laws as well to implement GLBA as it applies to the insurance business.

In addition to the regulations adopted by FFIEC member agencies, the FFIEC produced a December 2002 publication containing useful information security guidance (FFIEC Information Security Booklet). The FFIEC's mission is to develop common principles, standards, and report formats for the examination of financial institutions by federal examiners.[23] Examiners include in their reviews the information systems of financial institutions, and the FFIEC's publications provide IS examiners with useful guidance when performing the examinations. The FFIEC's December 2002 publication, a booklet called *Information Security (IT Examination Handbook)*, is intended as an update to the *1996 FFIEC Information Systems Examination Handbook*. The FFIEC Information Security Booklet contains control objectives (phrased as "shoulds") in a series of "Action Summaries," and each Action Summary is followed by useful explanations on various security topics. The FFIEC Information Security Booklet is helpful as guidance because it contains considerably more detail than GLBA or the regulations themselves. Together with the 1996 handbook, the booklet gives examiners objective criteria to help determine whether financial institutions are following "safety and soundness" standards. Financial institutions that do not meet safety and soundness standards are at risk of losing their charters to operate.

2. *What the GLBA Security Standards Say*

The Interagency Guidelines cover many of the typical financial institutions, such as banks, savings associations, and credit unions, whose regulators are members of the FFIEC.[24] The Interagency Guidelines provide guidance on various steps for developing and implementing a security program to protect customer information. At a high level, the Interagency Guidelines call for financial institutions to involve their boards of directors in their security programs; assess their risk; manage and control the risks identified; oversee arrangements with service providers; adjust the security program in light of new developments; and report to their boards at least annually concerning the results of the program.

Some security controls called for in the Interagency Guidelines to manage and control risk are of particular interest to financial institutions that transmit and store customer financial information in electronic form. These key required security controls are:

violations of "safety and soundness" standards are serious enough. As a practical matter, therefore, following the Guidelines is required for the institutions under OCC and FDIC oversight.

[21] The FFIEC also includes NCUA.

[22] These agencies are the Federal Trade Commission (FTC), NCUA, and the Securities and Exchange Commission (SEC). FTC security regulations appear at 16 C.F.R. part 314. NCUA's security regulations are at 12 C.F.R. § 748.0(b)(2). NCUA has added a modified copy of the Interagency Guidelines to the end of part 748, but the security controls are ones credit unions "should" implement, rather than controls they "shall" put in place. The SEC's security rule, part of Regulation S-P, appears at 17 C.F.R. § 248.30.

[23] Federal Financial Institutions Examination Council, "About the FFIEC – Mission," <http://www.ffiec.gov/about.htm>.

[24] As noted above, the FFIEC member agencies are the OCC, Federal Reserve Board, FDIC, OTC, and NCUA.

- **Access controls** on customer information systems.[25] The purpose of these access controls are to:
    - **Authenticate** individuals accessing customer information, and
    - **Permit access only to authorized individuals.**

- **Encryption** of electronic customer information. This requirement extends to customer information in transit or in storage on networks or systems, where unauthorized access is a threat to these networks or systems.[26]

- **Monitoring** of systems and procedures to detect actual and attempted attacks or intrusions affecting customer information.[27]

The security requirements for other types of financial institutions, appearing in other agencies' regulations, are more general than the requirements in the Interagency Guidelines.[28] Nonetheless, their provisions are consistent with the security controls in the Interagency Guidelines.[29]

The FFIEC Information Security Booklet expands on the general guidelines in the Interagency Guidelines by instructing examiners to look at the following controls:

- **The capability of updating access rights based on personnel or system changes**.[30]

- Consider **multi-factor authentication** for applications, "taking into account that multi-factor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities."[31]

- Consider the use of a **public key infrastructure** supporting **digital signatures** as a strong means of authentication.[32]

- **Encryption** implementation should include:
    - **Sufficient encryption strength**;

[25] Interagency Guidelines, Section III.C.1.a.

[26] Interagency Guidelines, Section III.C.1.c.

[27] Interagency Guidelines, Section III.C.1.f.

[28] For instance, the security provision in the SEC rule, Regulation S-P, 17 C.F.R. § 248.30, merely repeats GLBA's general statutory security objectives. FTC and NCUA regulations also contain provisions repeating these objectives. 16 C.F.R. § 314.3(b); 17 C.F.R. § 748.0(b)(2).

[29] For example, FTC regulations require risk assessments concerning and safeguards for "information processing, storage, transmission and disposal." 16 C.F.R. § 314.4(b)(2); *see also* 16 C.F.R. § 314.3 (safeguards must cover risk assessment elements described in section 31.4.4). Also, NCUA regulations reprint the Interagency Guidelines as an appendix to 12 C.F.R. part 748, and its version of the Interagency Guidelines is worded as non-binding guidelines.

[30] FFIEC Information Security Booklet, page 15.

[31] FFIEC Information Security Booklet, page 18.

[32] FFIEC Information Security Booklet, page 22.

- **Effective key management practices**;
- **Robust reliability**;
- **Appropriate protection of the encrypted communication's endpoints**.[33]

VOLTAGE SOLUTIONS PROTECT SENSITIVE FINANCIAL INFORMATION

Voltage Security provides a privacy platform that allows financial institutions to meet messaging security and privacy concerns head on. The Voltage Privacy platform enables organizations to protect their most sensitive financial services communications without building a complex infrastructure. Organizations can encrypt and send secure electronic financial information, internally or externally to customers and partners, without certificates, passwords, or the complexity of PKI.

The Voltage Privacy platform is based on award-winning technology – Identity-Based Encryption (IBE) –that eliminates the need for certificates, requires no change in end user behavior, can integrate with almost any network infrastructure, and enables security across a variety of channels controlled under a single policy framework.

Voltage SecureMail and SecureFile enable financial institutions to exchange sensitive information seamlessly, swiftly, and securely either with an integrated plug-in or without any software download. Voltage SecureMail Gateway enables Covered Entities to specify the policies that govern which messages will automatically be encrypted before being sent out. In addition Voltage SecureMail for the BlackBerry enables organizations to send and receive secure email using their mobile devices.

All Voltage security solutions contain the critical security technologies to enable customers to implement the safeguards mandated in GLBA. The table in the Appendix maps the security controls mandated in GLBA with security technologies that can address these controls, and shows how Voltage solutions use these technologies to protect customer information. No set of technologies provide complete GLBA security compliance "in a box." Yet using Voltage technology can play a critical role in an overall GLBA compliance program by securing different kinds of point-to-point communications and file management.

CONCLUSION

The financial system is one of the pillars of both our nation's and the world's economies. The financial services market is moving toward the use of the Internet for cost-savings and to provide new kinds of services not previously possible in the paper-based world. With these advances, however, come greater risks. GLBA requires financial institutions to address these risks with security standards established by federal and state regulators. The regulators have also created guidelines that will be used in evaluating the safety and soundness of financial institutions. Among these guidelines are security controls for authentication, encryption, and monitoring to detect attacks against systems. Voltage is a solutions provider whose secure mail, secure file transfer, and secure instant messaging technologies will enable financial institutions to transmit and store sensitive customer information securely, while helping them to enable secure online services to expand their markets and realize cost savings.

[33] FFIEC Information Security Booklet, page 48.

ABOUT VOLTAGE SECURITY

Voltage Security delivers the leading enterprise privacy management platform for protecting data privacy.

Based on an award-winning breakthrough in security and usability called Identity-Based Encryption (IBE), Voltage provides solutions for secure communication and data at rest to leading financial services, healthcare, government and pharmaceutical companies.

For companies concerned with complying with HIPAA, GLBA, PIPEDA, Basel II, SEC 17, SOX and SB1386, Voltage offers automated policy-based encryption that reduces the risks associated with privacy and compliance.

Voltage's Enterprise Privacy Management Platform provides a common framework for applying security and enforcing policies for data flowing inside and outside the enterprise, including email, files, documents, and instant messaging.

Voltage solutions secure data privacy by making anytime, anywhere security easy to use and painless to deploy.

For more information, please visit www.voltage.com, email info@voltage.com
or call +1 650 543 1280

Nothing in this white paper is to be construed as legal advice. You should address any legal questions to a qualified attorney.

Table 1 maps the technical GLBA security requirements and guidelines with the Voltage solution.

Technical Security Controls and Voltage's Solution for Financial Information

Type of Safeguard	Voltage Solution
Confidentiality and Access Control	
Access control on customer information. Controls to authenticate and limit access to authorized individuals.[34]	Voltage Privacy platform provides a management console for setting and administering policies, tracking key requests, and integrating with authentication or identity management solutions. No other solution offers the flexibility and control of authentication for people inside and outside the firewall.
Encryption of customer information, both while in transit and while at rest.[35] See Table 2 for detailed encryption guidelines in the FFIEC Information Security Booklet.	The Voltage Privacy platform enables organizations to easily encrypt and decrypt business communication without the burden of managing complex security information (e.g., certificates) for individuals. Voltage solutions permit the transmission of various communications to individuals or groups in an encrypted state, which only the authorized recipient(s) can decrypt. Furthermore, all content secured with Voltage solutions are stored encrypted wherever they may rest (e.g. mail server, portals, etc.)
The administration of access rights should include the ability to update access rights based on personnel or system changes.[36]	Because the Voltage IBE Server integrates with various identity management solutions (e.g. LDAP, Windows Active Directory, etc.), bank IT administrators can easily manage access rights. In contrast to other secure messaging solutions, the Voltage Security removes the need for administrators to replicate or create an additional user database for secure messaging.
Authentication	

[34] Interagency Guidelines, Section III.C.1.a; *see also* FFIEC Information Security Booklet, page 15.

[35] Interagency Guidelines , Section III.C.1.c.

[36] FFIEC Information Security Booklet, page 15.

Individuals must be authenticated to control access to only those persons authorized to see customer information.[37] Authentication methods should be appropriate to the level of risk.[38] Consider whether multi-factor authentication is appropriate for each application.	Voltage solutions permit financial institutions to issue a unique key pair to each user based in part on a simple identifier such as an email address. Voltage solutions leverage existing identity management solutions and provide the flexibility to choose and switch the form of centrally managed authentication. e.g. Active Directory, LDAP, email answerback authentication, Q&A authentication, or any custom authentication scheme that has been implemented.
Public key infrastructure, if implemented and maintained properly, is one option as a strong means of authentication.[39] See Table 2 for detailed guidelines in the FFIEC Information Security Booklet relating to the implementation of PKI.	Commonly called PKI, asymmetric systems were introduced to the market in the 1980s. In the PKI model, different keys—a public key and a private key—are used to encrypt and decrypt messages. Although PKI offers a strong means of authentication there are five critical shortcomings and flaws that exist in PKI that have prevented the technology from enabling ubiquitous secure messaging: 1. Certificates are not easily located. 2. Strict online requirement removes offline capability. 3. Validating policy is time-consuming and difficult to administer. 4. Certificates leak data. 5. User's must pre-enroll. Voltage's Identity-based Encryption overcomes the challenges in a PKI approach by eliminating the need for certificates while preserving public/private keys. This means huge usability improvements for end users and dramatically lowered administrative costs.
Security Management	
Systems holding customer information must have mechanisms to detect actual and attempted attacks on customer information.[40]	The Voltage IBE Server logs all server events. All logs can easily be viewed by administrators through the management console, or piped to a network management solution for immediate alerts on potential attacks.

[37] Interagency Guidelines, Section III.C.1.a.

[38] FFIEC Information Security Booklet, page 18.

[39] FFIEC Information Security Booklet, page 22-24.

[40] Interagency Guidelines, Section III.C.1.f; *see also* FFIEC Information Security Booklet, page 64 (implement logging for system components that warrant logging).

Table 2 discusses in detail the public key infrastructure and encryption guidelines in the FFIEC Information Security Booklet, and maps them to the capabilities of Voltage's security solutions.

PKI and Encryption Controls and Voltage's Solution for Financial Information

Type of Safeguard	Voltage Solution
Certificate Issuance and Revocation Policies	
Define Access control on customer information. Controls to authenticate and limit access to authorized individuals.[41]	The Voltage Privacy Platform provides banks the ability and flexibility to define policies controlling access to encrypted data. Access control policies may include, but are not limited to, defined security settings for client application, variable authentication policies for diverse groups, and frequency management of mandatory re-keying and/or re-authentication.
Select an appropriate certificate validity period.[42]	Voltage solutions address the important need for key revocation without the burdens associated with certificates. Keys are automatically revoked after a predefined time period (e.g. weekly) providing Security Officers better control over risk exposure associated with issued keys.
The application should ensure that a digital certificate is valid before relying on it, through mechanisms such as a certificate revocation list.[43] Define the circumstances for authorizing a certificate revocation, such as private key compromise or closing the user's account.[44] Updating the database of revoked certificates frequently, ideally in real time.[45]	Voltage solutions address the important need for key revocation without the burdens associated with digital certificates. Because Voltage Security solutions do not use traditional Public Key certificates for encrypting data, banks do not need to deploy expensive certificate revocation lists. The Voltage IBE Server integrates with various identity management solutions (e.g. LDAP, Windows Active Directory, etc.), bank IT administrators can easily remove private key access revoking access rights in real-time. The stateless nature of the server makes it scalable as well as easier to manage than any other PKI system. No key directory, no user directory, no message repository.

[41] FFIEC Information Security Booklet, page 23.

[42] FFIEC Information Security Booklet, page 23.

Stringent measures to protect the root key.[46]	Voltage provides a set of best practices to protect the Master secret. Future implementations will include support for HSM.
Regular independent audits.[47] Recording in a secure audit log all significant events in the certificate lifecycle.[48] Regularly reviewing exception reports and system activity to detect unauthorized activities.[49]	The Voltage IBE Server logs private key requests, key generation, key revocation, and key changeover events to assist in bank audits and reviews. A separate log keeps track of all administrative actions. All logs can easily be viewed anytime, by bank auditors through the management console, or piped to a network management solution.
Adhering to CA and authentication systems with "widely accepted PKI standards" to maximize inter-enterprise acceptability of certificates.[50]	Voltage's products are based on well-known cryptographic standards such as AES, SHA-1, and 3DES, and Voltage's secure messaging format is based on the widely accepted S/MIME standard. In addition The Voltage Security platform integrates easily into existing PKIs, such as the Federal Trust Bridge, by chaining up to existing Certificate Authority trust hierarchies. All of the benefits associated with traditional PKI can be extended across the client environment using IBE, without the need for digital certificates to be issued and managed for every client.

[43] FFIEC Information Security Booklet, page 23.

[44] FFIEC Information Security Booklet, page 23.

[45] FFIEC Information Security Booklet, page 24.

[46] FFIEC Information Security Booklet, page 24.

[47] FFIEC Information Security Booklet, page 24.

[48] FFIEC Information Security Booklet, page 24.

[49] FFIEC Information Security Booklet, page 24.

[50] FFIEC Information Security Booklet, page 24

Encryption controls	
Encryption strength sufficient to protect the information from disclosure until the disclosure poses no material risk.[51]	The strength of the encryption currently used in Voltage’s products is equivalent to 1024-bit RSA. Voltage’s products are based on well-known cryptographic standards such as AES, SHA-1, and 3DES, and Voltage’s secure messaging format is based on the widely accepted S/MIME standard. Voltage’s products are currently undergoing FIPS validation by NIST to ensure compliance with cryptographic standards.
Effective key management controls.[52]	Voltage’s Identity-based Encryption (IBE) makes it easier to manage keys then PKI. With the ability to automatically generate or determine keys, IBE does away with certificate revocation lists (CRLs) and various life cycle tasks, such as key escrow. IBE handles policy and management dynamically, meeting the requirements addressed by the FFIEC for effective key management.
Robust reliability, such as with the products used and administrative controls.[53]	Unlike traditional approaches to encryption, the Voltage solutions is very light weight in terms of administrative overhead, the solution scales without requiring additional moving parts and end users are not affected if servers are off-line. It is very easy to add additional server capability for redundancy purposes as well as in a disaster recovery scenario.
Appropriate protection of the encrypted communication endpoints.[54]	With the Voltage Privacy Platform emails are secured in transit and at rest: Emails are secured (encrypted and signed) on the desktop and securely passed through the enterprise’s email server. Once the recipient is authorized he/she decrypts the message on or offline, reads the message and attachments, and then the sensitive data is re-encrypted for storage. Government and corporate compliance requirements are

[51] FFIEC Information Security Booklet, page 48.

[52] FFIEC Information Security Booklet, page 48.

[53] FFIEC Information Security Booklet, page 48.

	fulfilled as messages are secured not only in storage on the mail server but as it leaves the corporate firewall.
Encryption key management	
Generating keys for different cryptographic systems and different applications.[55]	The Voltage Privacy Platform provides administrators the ability to easily secure multiple communication applications through one single framework. Furthermore, the Voltage IBE Toolkit will also allow banks to build and manage their own secure applications through the same framework.
Generating and obtaining public keys.[55] Distributing keys to intended user.[56]	Voltage's Privacy Platform utilizes users' identities (e.g., email addresses or network logins) as their public key, and directs users to obtain their private key from a trusted source. This seemingly simple but technically difficult breakthrough makes certificates superfluous and ties security policy directly to the encryption or authentication method. This process makes key distribution easy for the administrator and transparent to the end user.
Storing keys.[57]	The Voltage IBE Server generates private keys, on demand from a master secret so keys do not have to be stored or archived. Thus any information protected with the Voltage solution can be recovered at any time. Additional servers -- such as Certificate Authorities, Certificate Directories, Email Storage Servers, and Key Storage Servers -- often associated with PKI or other secure messaging solutions are not needed.

[54] FFIEC Information Security Booklet, page 48.

[55] FFIEC Information Security Booklet, page 50.

[55] FFIEC Information Security Booklet, page 50.

[56] FFIEC Information Security Booklet, page 50.

[57] FFIEC Information Security Booklet, page 50.

Changing or updating keys.[58] Dealing with compromised keys and revoking keys.[59]	Voltage solutions address the important need for key revocation without the burdens associated with certificates. Keys are automatically revoked after a predefined time period (e.g. weekly) providing Security Officers better control over risk exposure associated with issued keys.
Recovering keys that are lost or corrupted.[60] Archiving and destroying keys.[61]	One important infrastructure requirement for enterprise customers in regulated industries is the ability to easily implement disaster recovery. Because the Voltage IBE Server is a stateless server, it does not need to store any decryption keys. This means that all information needed for Disaster Recovery needs to be backed up only once during installation.
Logging the auditing of key management-related activities.[62]	The Voltage IBE Server logs private key requests, key generation, key revocation, and key changeover events to assist in bank audits and reviews. In addition, administrator logs can easily be accessed to detect unauthorized activities. All logs can be viewed through the management console, or piped to a network management solution.
Instituting defined activation and deactivation dates, limiting the usage period for keys.[63] Keys should be changed frequently.[64]	Voltage solutions address the important need for key revocation without the burdens associated with certificates. Keys are automatically revoked after a predefined time period (e.g. weekly) providing Security Officers better control over risk exposure

[58] FFIEC Information Security Booklet, page 50.

[59] FFIEC Information Security Booklet, page 50.

[60]

[61] FFIEC Information Security Booklet, page 50.

[62] FFIEC Information Security Booklet, page 50.

[63] FFIEC Information Security Booklet, page 50.

[64] FFIEC Information Security Booklet, page 51.

	associated with issued keys.
Key management is fully automated and takes place without the ability for personnel to influence the process.[65]	The Voltage Privacy Platform conducts key management (key generation, key issuance and policy enforcement) automatically behind the scenes, removing the need for administrators to be constantly watching over the solution. Other secure messaging solutions (e.g. PKI) require large number of servers with heavy administrator involvement.
No private keys are ever exposed in an unencrypted state.[66]	The Voltage IBE Server, which is responsible for private key generation, generates private keys on-demand – no private keys are stored on the server. This ensures that no private keys are ever exposed in an unencrypted state. Key issuance is conducted over secure SSL connection also ensuring that keys are protected in transit.
Keys are randomly chosen from the entire key space, preferably by hardware.[67]	Keys generated by Voltage solutions are based on the entire key space and are provably not susceptible to collusion attacks, ensuring the highest level of security of information.
Key-encrypting keys are separate from data keys.[68]	All keys are generated on an as needed basis by authorized users, the Voltage solution eliminates the need to issue separate keys

[65] FFIEC Information Security Booklet, page 50.

[66] FFIEC Information Security Booklet, page 50.

[67] FFIEC Information Security Booklet, page 50.

[68] FFIEC Information Security Booklet, page 50.

All patterns in clear text are disguised before encrypting.[69]	During the Voltage encryption process of information, patterns in clear text are removed to ensure that it is not susceptible for cryptographic attacks.
Keys with a long life are sparsely used.[70]	Voltage solutions address the important need for key revocation without the burdens associated with certificates. Keys are automatically revoked after a predefined time period (e.g. weekly) providing Security Officers better control over risk exposure associated with issued keys.
Keys that are transmitted are sent securely to well-authenticated parties.[71]	Voltage's Privacy Platform utilizes users' identities (e.g., email addresses or network logins) as their public key, and directs users to obtain their private key from a trusted source. This seemingly simple but technically difficult breakthrough makes certificates superfluous and ties security policy directly to the encryption or authentication method. This process makes key distribution easy for the administrator and transparent to the end user.
Key generating equipment is physically and logically secure throughout its lifecycle.[72]	Voltage provides customers recommendations on best practices to how to protect their Voltage Security solution.

[69] FFIEC Information Security Booklet, page 50.

[70] FFIEC Information Security Booklet, page 51.

[71] FFIEC Information Security Booklet, page 51.

[72] FFIEC Information Security Booklet, page 51.