949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

Security Issues Facing Financial Institutions (and their suppliers & partners)

- Regulations
- Customer Confidence related to On-line transaction security
- Security threats

Banking Industry IT Security Compliance Objectives

Administrative, Technical, and Physical Safeguards that provide security, confidentiality, integrity and proper disposal of customer information.

IT Security Areas of Focus

- Adherence to "Best Practices" in security for requiring risk assessment, controls, appropriate IT Infrastructure, internal processes and reporting as outlined by the Federal Gramm-Leach-Bliley Act (GLBA section 501b)
- Proper control of and identification of parties who have access to private consumer data

Financial Institution Regulations

Regulation	Summary Information	Applicable Institutions
1. FFIEC & FDIC (10/12/05) & NUC (Credit Unions) **Guidelines Related to "Authentication in an Internet Banking Environment"**	**Purpose** *To Provide effective methods to authenticate the identity of customers using internet based products & services.* **Regulations** Financial institutions regulated by the agencies should conduct: • Perform **Risk-based assessments**, • Develop ***Customer Awareness*** programs • Develop **security measures to *reliably authenticate customers*** *remotely accessing their Internet-based financial services* • **Two-Factor Authentication is Required by Dec. 2006 for High Risk Internet Transactions** • Account Origination & Customer Verification – See Patriot Act • **Monitoring & Reporting** – to determine unauthorized access to information. *Multi-layers* of Control. *Reporting* on activities. **Independent party review** on security activities. **Penalties & Enforcement** Regulation by agencies for each financial institution (FTC, State Insurance Regulators, SEC…), plus certain regulations carry fines, imprisonment or threats of lawsuits.	• **Financial institutions offering Internet-based products and services to their customers** • **FDIC supervised banks** (Commercial & Savings) • **Partners, Suppliers**
2. FFIEC & FDIC	**Compliance with Federal and State regulations and other security guidelines as outlined by FFIEC IT Security Audit Booklets**	• **Financial Institutions regulated by FFIEC**

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

Regulation	Summary Information	Applicable Institutions
3. **GLBA**	**Purpose** Protection of Non-Public personal information by financial institutions and their partners **Regulations** • Administrative, Technical & Physical Safeguards ○ Ensure Security & Confidentiality of Customer Information ○ Protect against anticipated Threats ○ Protect against unauthorized access to such records – harm or inconvenience	**All 9,500+ Financial Institutions: Securities, Banks, Insurance Firms**
Section 501 a & b	• Administrative, Technical & Physical Safeguards ○ Ensure Security & Confidentiality of Customer Information ○ Protect against anticipated Threats Protect against unauthorized access to such records – harm or inconvenience	
Section 502	**May not Disclose personal information to any non-affiliated 3rd party** unless that party is in compliance with Section 503 (Consumer permission). Exceptions apply.	
Section 503	**Annually and with new customer relationships, institutions must disclose to customers policies re:** • Disclosing non-public information and • Practices for protecting non-public personal information.	
Section 504	**Must be compliant with the appropriate regulatory agencies for each type of institution.**	
Section 505, 522	**Enforcement is from the appropriate regulatory agency which must create rules for compliance with this Act** (FTC, SEC, State Insurance Agencies, FDIC [banks], National Credit Union Administration [Credit Units] and Fed. Banking agencies).	
Section 521	**Privacy Protection – Obtaining customer information using false pretenses**	
Section 523	**Criminal Penalties for knowingly violating Section 521 (5 Years or fine)**	
Summary	**Institutions must have a stated plan for protecting customer information, adhere to related regulatory agency rules, inform customers, and Implement appropriate security measures.**	
4. **FACT Act** (2003) Section 216	**Purpose** Accuracy and Fairness in Credit Reporting Designed to enhance the quality of Consumer credit information, protect against Theft **Regulations for Lenders** • Use Red Flag indicators to identify identity thieves Proactively adhere to credit agency guidelines related to identity theft patterns	• Credit Reporting Agencies • **Banks** & other Suppliers & Users of Credit Information
5. **U.S. Patriot Act** Sect. 312, 326 10/26/01, 1/4/06	**Purpose** Anti-Terrorism **Applicable Financial Regulations Below (Identity Verification)** • International Money Laundering Abatement • Verification of Identity – New Accounts	

Regulation	Summary Information	Applicable Institutions
6. California SB 1386 (July 2003)	**Purpose** To protect the privacy of consumer private information. **Regulation** Organizations must warn California residents of any security breach of unencrypted "Personal Information " **Penalties** Public disclosure, law suits, loss of business	**Any California company** that has in its possession "Personal Information"
7. 46 U.S. State Laws (as of 2/09)	**Purpose** To protect the privacy of consumer private information. **Regulation** Varies -- Organizations must warn residents of any security breach of unencrypted "Personal Information " **Penalties** Varies -- Public disclosure, lawsuits, loss of business	**Any company** existing in a regulated state that has in its possession "Personal Information"
8. Sarbanes-Oxley Act of 2002 (SOX)	**Purpose** Sarbanes-Oxley Act (SOX) was designed to **restore investor confidence following the outbreak of corporate scandals and bankruptcies around 2000**. Currently SOX is only applicable to publicly traded companies under jurisdiction of SEC, but some states are pushing for application to large non-profit organizations. **Regulation:** Sarbanes-Oxley Act called for the creation of the *Public Company Accounting Oversights Board.* This board will register and regulate all public accounting firms, including inspections of accounting firms, investigations and disciplinary proceedings, and enforce compliance with professional standards. SOX also outlines the responsibilities of the accounting firms: • **Section 204**- Auditors must report all critical accounting policies and practices to the firm's audit committee. • **Section 203**- The lead audit and reviewing partner must rotate off the audit every 5 years. • **Section 201**- Prohibits any public accounting firm from providing non-audit services while auditing firm. These services include bookkeeping, appraisal, and others (excludes tax preparation). • **Section 301** calls for the formation of an independent and competent audit committee. The audit committee is responsible for hiring, setting compensation, and supervising the auditor's activities. • **Section 302** requires the CEO and chief financial officers to certify that the financial statements accurately and fairly represent the financial condition and operations of the company. There are criminal sanctions for intentional false certification. • **Section 402** prohibits loans to any of the firm's directors or executives. • **Section 409** requires rapid disclosure of material changes in the financial conditions of the firm. • **Section 404** requires that each annual report contain an **internal control report**. This report states the responsibility of	Public Companies

Regulation	Summary Information	Applicable Institutions
	management for establishing and implementing adequate procedures for financial reporting. This report must include: assessment of effectiveness of internal control structure and procedures, any code of ethics and contents of that code. Companies must protect sensitive data like: medical and financial information and customer data such as SSN's, Tax id numbers, credit information and bank records. • **Whistle Blower Protection** • **Section 1102** makes it a crime for any person to destroy, alter, or conceal any document to prevent its use in official legal proceedings.	
9. The Fair Credit Reporting Act ("FCRA") **(1970)**	Enacted to protect consumers from the disclosure of inaccurate and arbitrary personal information held by consumer reporting agencies. Under the FCRA, consumer reporting agencies may only disclose personal information to third parties under specified conditions.	Consumer reporting Agencies
10. Right to Financial Privacy Act (1978)	Designed to protect the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. Prevents banks from requiring customers to authorize the release of financial records as a condition of doing business and states that customers have a right to access a record of all disclosures.	Financial Institutions

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

All Companies (Federal Rules of Civil Procedure – FRCP)

Regulation	Summary Information	Applicable Institutions
1. FRCP (12/1/06) **Federal Rules of Civil Procedure**	**Purpose** *Requires companies to manage their electronic data so that it can be produced in a timely manner (Emails, IM, Files, documents).* **Regulations** a. Email/IM & document archiving with timely electronic data discovery (by topic as requested) b. Data retention policies c. The definition of "Reasonably accessible data" is up to the courts **Penalties & Enforcement** Federal courts can impose penalties for non-compliance, plus court case losses can result from not having the proper information to rebut allegations.	**All Companies that might ever be involved in a Federal legal matter. Also applies to law suits that cross state lines and is starting to be adopted by States as well.**

Consumer Information Privacy & Breach Regulations

Regulation	Summary Information	Applicable Institutions
1. GDPR **General Data Protection Regulation** (5/2018)	**Purpose** To provide consumers control of all their personal data when interacting with companies. **Regulation** **Companies must provide transparent information, communication and systems to exercise the rights of the data subject.** • Consent to use data • Controller & Processing Information • Right to Access Data • Right to Rectification • Right to Erasure • Right to Restrict Processing • Right to Control Your Data & Portability • Right to Object • Right to Compensation (in cases of misuse) **Penalties** Compliance is enforced by **fines** up to 4% of WW annual revenue or **20M Euros** whichever is higher.	**All European companies or companies dealing with European consumers**
2. California CCPA **California Consumer Privacy Act** (6/2018)	**Purpose** To provide consumers control of all their personal data when interacting with companies. **Regulation** Requires businesses collecting information about California consumers to appropriately and securely manage private data and manage the relationship with the consumer so that the consumer has control and visibility of their data. • Provide Transparency in The Collection of Personal Information • Deletion of Personal Information • Right to Access Your Data • Right to Control Your Data **Penalties** Consumers may seek statutory damages of $100 to $750 per incident.	**All California Companies that are over a defined size**

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

Regulation	Summary Information	Applicable Institutions
	The other rights embodied in the CCPA may be enforced only by the Attorney General—who may seek civil penalties up to $7,500 per violation.	
3. California SB 1386 (July 2003)	**Purpose** To protect the privacy of consumer private information. **Regulation** Organizations must warn California residents of any security breach of unencrypted "Personal Information " **Penalties** Public disclosure, lawsuits, loss of business	**Any California company** that has in its possession "Personal Information"
4. 50 U.S. State Laws (as of 2018)	**Purpose** To protect the privacy of consumer private information. **Regulation** Varies -- Organizations must warn residents of any security breach of unencrypted "Personal Information " **Penalties** Varies -- Public disclosure, lawsuits, loss of business	**Any company** existing in a regulated state that has in its possession "Personal Information"
5. Credit Card (Payment Card Industry PCI) Regulations **(See PCI Section)**	**Purpose** Protect consumer private financial information and generate merchant trust **Regulations** Increasing requirements depending on the number of transactions or $$ per month **Penalties** Fines, restrictions from payment card system or permanent expulsion and potential public disclosure	**Online merchants** **Non-online merchants may soon be regulated too**

6. All Financial Industry Regulations (See Reg. summary)	**Purpose**
	Protection of Non-Public personal information by financial institutions & their partners
	Regulations
	• Administrative, Technical & Physical Safeguards
	  ○ Ensure Security & Confidentiality of Customer Information
	  ○ Protect against anticipated Threats
	Protect against unauthorized access to such records – harm or inconvenience
		• **Financial institutions offering Internet-based products and services to their customers**
		• **FDIC supervised banks** (Commercial & Savings)
		• **Partners, Suppliers**

7. Privacy Act of 1974	The Privacy Act of 1974 was designed to protect individuals from an increasingly powerful and potentially intrusive federal government. The statute was triggered by the report published by the Department of Health, Education and Welfare (HEW), which recommended a "Code of Fair Information Practices" to be followed by all federal agencies.	**Federal Agencies**
8. Other Privacy Acts	Privacy rights to protect other specific kinds of information. • Privacy Protection Act of 1980 • Cable Communications Policy Act of 1984 • Electronic Communications Privacy Act (1986) • Video Privacy Protection Act of 1988 • Telephone Consumer Protection Act of 1991 • Driver's Privacy Protection Act of 1994 • Communications Assistance for Law Enforcement Act of 1994	

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

Regulation	Summary Information	Applicable Institutions
	• Telecommunications Act of 1996 • Children's Online Privacy Protection Act (COPPA) of 1998	

While currently there is no national law to protect the privacy of the information you share online, federal law and state law do offer some protection to various kinds of personal information collected about you. At the national level, Congress has enacted laws as it perceived the need to arise. Therefore, you will see from the list below that you have

Education Institution Regulations

Regulation	Summary Information	Applicable Institutions
FERPA (12/08)	**Purpose** To protect the privacy of student records. **Regulation** Must obtain signed, written permission from the student before sharing educational record information **Penalties** Withhold federal funding, Lawsuits	**Any educational institution receiving funds from the federal government**
CIPA (2001)	**Purpose** To protect minors from internet access, mail/chat/IM and inappropriate or harmful matter. No authorized dissemination of minor personal data. **Regulation** Monitor, block, filter online activities to enforce purpose **Penalties** Withhold federal funding, Lawsuits	**Any school or library that gets federal internet access funding**

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

HIPAA - Health Insurance Portability & Accounting Act of 1996 (Final 2-20-03)

Regulation	Summary Information	Applicable Institutions

HIPAA	**Purpose**
	Safeguarding of electronic protected health information (EPHI)
	Covers:
	• Electronic transactions and code sets standards requirements
	• Privacy requirements
	• Security requirements
	• National identifier requirements
	
	Administered by the Centers for Medicaid & Medicaid Service (CMS)
	
	Compliance & Penalties:
	• **Administered by the CMS**
	• **Deadlines:**
	  • **April 2005 or 2006 (in effect now)**
	• **Compliance Driven by Complaints**
	• **Penalties:**
	  • **Transaction Violations:** Up to $100/ person per violation
	  • **Standard violations:** Up to $25,000/ person per violation per year
		• Covered Health Care Providers
		• Health Plans
		• Health Care Clearinghouses
		• Medicare Prescription Drug Card Sponsors

Summary	**Includes the following Security Regulations** **Administrative Safeguards** • Security Management Process (164.308(a)(1)) • Assigned Security Responsibility (164.308(a)(2)) • Workforce Security (164.308(a)(3)) • Information Access Management (164.308(a)(4)) • Security Awareness and Training (164.308(a)(5)) • Security Incident Procedures (164.308(a)(6)) • Contingency Plan (164.308(a)(7)) • Evaluation (164.308(a)(8)) • Business Associate Contracts and Other Arrangements (164.308(b)(1)) **Physical Safeguards** • Facility Access Controls (164.310(a)(1)) • Workstation Use (164.310(b)) • Workstation Security (164.310(c)) • Device and Media Controls (164.310(d)(1)) **Technical Safeguards** • Access Control (164.312(a)(1)) • Audit Controls (164.312(b)) • Integrity (164.312(c)(1)) • Person or Entity Authentication (164.312(d)) • Transmission Security (164.312(e)(1)) **Organizational Requirements** • Business Associate Contracts or Other Arrangements (164.314(a)(1)) • Requirements for Group Health Plans (164.314(b)(1)) **Policies and Procedures and Documentation** • Policies and Procedures (164.316(a))	

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

HITECH Act - The Health Information Technology for Economic and Clinical Health Act (HITECH Act or "The Act") is part of the American Recovery and Reinvestment Act of 2009 (ARRA).

Regulation	Summary Information	Applicable Institutions

HITECH	**Purpose**
	Improved privacy and Provisions for HIPAA
	Covers:
	13401 Application of security provisions and penalties to business associates of covered entities; annual guidance on security provisions.
	13402 Notification in the case of breach.
	13403 Education on health information privacy.
	13404 Application of privacy provisions and penalties to business associates of covered entities.
	13405 Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format.
	13406 Conditions on certain contacts as part of health care operations.
	13407 Temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities.
	13408 Business associate contracts required for certain entities.
	13409 Clarification of application of wrongful disclosures criminal penalties.
	13410 Improved enforcement.
	13411 Audits.
	
	Administered by the Centers for Medicaid & Medicaid Service (CMS)
	
	Compliance & Penalties:
	• **Administered by the CMS**
	• **Deadlines:**
	  • **April 2010 (in effect now)**
	• **Compliance Driven by Complaints**
	• **Penalties:**
	  • **Transaction Violations:** Up to $100/ person per violation
	  • **Standard violations:** Up to $25,000/ person per violation per year
		• Covered Health Care Providers
		• Health Plans
		• Health Care Clearinghouses
		• Medicare Prescription Drug Card Sponsors

949-261-5555
Newport Beach, Ca. 92660
www.eSecuritySolutions.com

PCI (Payment Card Industry) Data Security Standard (DSS)

<table>
<tr><th>Regulation</th><th>Summary Information</th><th>Applicable Institutions</th></tr>
<tr>
<td>PCI Data Security Standard (DSS)</td>
<td>
Purpose
The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.
<table>
<tr><th>Goals</th><th>PCI DSS Requirements</th></tr>
<tr><td>Build and Maintain a Secure Network</td><td>1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters</td></tr>
<tr><td>Protect Cardholder Data</td><td>3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks</td></tr>
<tr><td>Maintain a Vulnerability Management Program</td><td>5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications</td></tr>
<tr><td>Implement Strong Access Control Measures</td><td>7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data</td></tr>
<tr><td>Regularly Monitor and Test Networks</td><td>10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes</td></tr>
<tr><td>Maintain an Information Security Policy</td><td>12. Maintain a policy that addresses information security for employees and contractors</td></tr>
</table>
Tools for Assessing Compliance
Qualified Assessors. The Council manages programs that will help facilitate the assessment of compliance with PCI DSS: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are approved by the Council to assess compliance with the PCI DSS. ASVs are approved by the Council to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers.
ASVs – An Approved Scanning Vendor (ASV) is a data security firm using a scanning solution to determine whether or not the customer is compliant with the PCI DSS external vulnerability scanning requirement. ASVs have been trained and are qualified by the PCI Security Standards Council to perform network and systems scans as required by the PCI DSS.
Self-Assessment Questionnaire. The “SAQ” is a validation tool for organizations that are not required to undergo an on-site assessment for PCI DSS compliance. Different SAQs are specified for various business situations. The organization’s acquiring financial institution can also determine if it should complete a SAQ.
Depending on an organization’s classification or risk level (determined by the individual card brands), processes for validating compliance and reporting to acquiring financial institutions usually follow this track:
1. PCI DSS Scoping – determine what system components are governed by PCI DSS
2. Sampling – examine the compliance of a subset of system components in scope
3. Compensating Controls – QSA validates alternative control technologies/processes
4. Reporting – merchant/organization submits required documentation
5. Clarifications – merchant/organization clarifies/updates report statements (if applicable) upon bank request
Penalties:
Increasing requirements depending on the number of transactions or $$ per month
</td>
<td>All merchants who accept or process payment cards</td>
</tr>
</table>