An Overview of Customer Data Privacy Regulation In the Financial Services Sector

In the last eight years alone, there have been eight new Federal laws targeting financial services entities, making financial services the most highly regulated sector. More specifically, much of this legislation is concerned with the protection of non-public information (NPI) and personally identifiable information (PII). With major customer data breaches reported by the media on a daily basis, and with identity theft as the fastest growing financial crime, it is not surprising that regulators are focusing their attention on this growing issue. Even more legislation is on the horizon.

Understanding these data protection laws is no simple matter. Each law typically contains hundreds of pages of information and legal jargon, and can each take many hours to read and comprehend. Furthermore, correct interpretation – understanding how, when, and to whom they apply – can be a significant hurdle for any size institution, not to mention developing and implementing solutions to aid compliance. Many small to midsize institutions, who do not always have technical expertise in-house, often struggle with what is required for compliance. Without specialized skills, it is not surprising that many organizations have an incomplete understanding of their duties for meeting compliance. It can be a “hit or miss” process in many cases, resulting in greater scrutiny and even fines and penalties from regulators including the Federal Financial Institutions Examination Council (FFIEC), the Securities and Exchange Commission (SEC), the Federal Trade Commission (FTC), and other agencies.

The purpose of this whitepaper is to give an overview of data privacy laws that are applicable to the protection of non-public information (NPI) and its counterpart, personally identifiable information (PII). Because of complexity, this white paper is not intended as a single source for implementing compliance strategies. Rather, the paper serves to highlight regulations for further investigation. In addition, it will also illustrate how Intrusion’s Compliance Commander data protection products serve to help meet regulatory compliance.
Non-Public Information and Personally Identifiable Information

Non-public information (NPI) is an encompassing term that refers to all information appearing on applications for obtaining financial services (credit card or loan applications), or on account histories (bank or credit card). It also includes the customer’s status with the organization: either a current or previous customer. NPI can include: names, addresses, telephone numbers, Social Security numbers, PINs, passwords, account numbers, salaries, medical information, and account balances. In general, NPI is broader than its counterpart, personally identifiable information (PII).

PII is typically regarded in the information security and privacy fields as any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. PII can include: national identification numbers, street addresses, driver’s licenses, telephone numbers, IP addresses, email addresses, vehicle registrations, and ages.

While identity theft is the number one financial crime in the United States, the theft of intellectual corporate data is also on the rise. Out of the last eight Federal laws enacted three specifically mandate financial services entities to protect customer personal information and to combat identity theft: GLBA, the Identity Theft and Assumption Deterrence Act, and the USA Patriot Act. In addition, 23 states have passed data protection laws, which also apply to financial services organizations. The remaining laws relate to protecting intellectual corporate data and information assets, but the same security safeguards apply to all.

Popular Misconceptions of Regulations

Because of their complexity, it is easy to understand why misconceptions about regulations are frequently found in the financial services sector. Following are a few examples of these misconceptions:

- **Gramm-Leach-Bliley Act (GLBA)** - Early on, financial institutions were under the misconception that GLBA only involved privacy notifications and the opt in/out requirements for sharing of information with non-affiliated parties. Many organizations were not implementing the information security program requirements for protecting NPI.

- **Sarbanes-Oxley Act (SOX)** - At one stage, SOX was once thought to only be a financial regulation and not have any ties to information technology; however, information systems are the backbone of financial applications and processes, and are used to originate, house, store, and transmit financial information.

- **CA SB1386, and other state data protection laws** - Many organizations have inaccurately evaluated the applicability of the individual state data protection laws to their businesses because they were not physically located in that state. The majority of the state laws dictate that if a business has customers that are residents of the enforcing state, the law applies to that business regardless of whether or not the business is physically located in the enforcing state. Many of the laws also exempt from disclosure encrypted information that is stored or transmitted.
Regulations for the Protection of NPI and PII

To give a quick overview of the regulatory landscape, listed below are the relevant regulations which must be observed for the protection of NPI and PII. Compliance with these various regulations is typically determined during a regulatory examination, or if a security breach/compromise is reported.

**Gramm-Leach-Bliley Act Data Protection Act of 1999 (GLBA)** – Section 501(b) of GLBA requires financial services companies to protect the confidentiality and integrity of NPI, and to ensure it is secure from unauthorized access. In order to do so, organizations must identify potential threats to their information and implement controls which include: policies, procedures and technologies. These technologies include monitoring and detection systems for actual and attempted actions for gaining access to NPI. Noncompliance with GLBA may result in:

- civil monetary fines of varying amounts up to $1 million or more,
- prison sentences of up to five years,
- lower examination ratings and increased reporting requirements, and
- enforcement actions, which can include board resolutions, memorandums of understanding, written agreements, and cease and desist orders.

The specific action is based upon the number of deficiencies, risk profile, and whether or not violations have been encountered (such as transmitting unencrypted information to third parties, such as programmers, credit bureaus, loan processors, or other service providers).

**Identity Theft and Assumption Deterrence Act of 1998** – This Act was created to address the growing problem of identity theft in the U.S. and it addresses:

- the fraudulent creation, use or transfer of identification documents, and
- the theft and/or criminal use of the underlying personal information.

It applies to anyone who knowingly transfers or uses NPI or PII with the intent to commit, or aid and abet any unlawful activity. While identity theft can occur through a variety of means, unprotected electronic communications is a primary target. Therefore, electronic communications should be subject to content monitoring and filtering to lessen the potential for data leakage through these network channels. Violations of the Act are generally subject to a fine and/or imprisonment of up to 15 years. Specific actions are determined at the time when the infraction is reported, or during a regulatory examination.

**The USA Patriot Act** – Section 314 of this regulation requires financial institutions to implement prudent steps to protect the confidentiality of NPI. Proactive monitoring and auditing of electronically transmitted information is required for alerting organizations to: unauthorized access, unauthorized sharing, or other compromises of protected information. The integrity and protection of NPI is imperative for the monitoring and investigation of money laundering and terrorist financing. Fines in an amount not more than 3 times the monetary equivalent of the thing of value, or imprisonment up to 15 years, or both may be assessed for violations of this Act.

**Sarbanes-Oxley Act of 2002 (SOX)** – Section 404 of SOX mandates that publicly traded companies implement and maintain internal controls for the protection of corporate financial information, and for the timely detection of unauthorized access, insider abuse and unauthorized sharing of the information. Organizations found in noncompliance will be subject to substantial fines of up to $1 million and sentences of up to 10 years in prison.

**NASDAQ** – The NASD has implemented various regulations and guidance on the use of electronic communications for transmitting NPI, PII, corporate confidential data, misleading or insider information, or inappropriate solicitations or guarantees. The NASD rules require the monitoring and review of content for all outgoing messages. Fines of varying amounts up to $1 million and sanctions may be assessed for noncompliance.
CA SB1386 and AB 1950, State Data Protection Laws – As of January 1, 2006, 23 states have passed data protection laws which require organizations that electronically collect and maintain NPI and PII, to implement security controls and to protect the confidentiality of the information through various safeguards including monitoring and reporting systems. A national law is under debate. If data is compromised, organizations must notify all customers. Failure to do so may result in lawsuits and regulatory penalties.

Basel II – Operational Risk – Basel II proposes a new capital adequacy framework for institutions who demonstrate proactive risk management strategies associated with operational risks. Risk management strategies are to include policies and practices for controlling and mitigating operational risks. The protection of information assets, which would include the monitoring and reporting of unauthorized access and sharing, will be necessary to comply with the requirements. The federal agencies are retaining current prompt corrective actions and capital requirements.

European Union Privacy Directive – Similar to the U.S. GLBA, the EU Privacy Directive addresses the protection and confidentiality of NPI. The requirements under the EU Privacy Directive closely mirror those of GLBA, requiring adequate measures to safeguard the information from unauthorized access and unauthorized sharing, whether the data is at rest or in-transit. Entities found in noncompliance may be subject to fines and sanctions, established by each EU Member.

Payment Card Industry (PCI) Security Standards – PCI security requirements, issued by MasterCard and Visa, went into effect in July 2005. These standards apply to merchants and financial institutions whom accept credit card transactions. All entities that accept credit cards must encrypt all transmissions of cardholder data, and implement logging and monitoring, among other controls. Noncompliance can result in fines of up to $500,000 per incident if card data is compromised.

Implementing a Proactive Security Strategy

Electronic communications have become an essential and effective channel for organizations to conduct business. However, along with the ease of transacting business and the global reach it provides, also comes the risk of data leakage While there is no silver bullet for protecting information assets from the risks and threats of leakage, a proactive security program which encompasses prudent practices, such as content monitoring and filtering of electronic communications, will help ensure the security and confidentiality of NPI and PII, and compliance with regulations that mandate the protection of sensitive information. Regulatory compliance must be achieved; however, it shouldn’t be the only reason for implementing proactive security.

Security controls instill confidence and trust; and these practices show your customers that you value their business and respect their privacy needs. Security controls also protect your reputation by limiting your vulnerability to security threats and data compromises, thereby helping you attract new business and improve your bottom line. Not instituting proactive tools for monitoring, reporting, and controlling the risk of unauthorized access or disclosure, puts your institution at a serious risk for compromise, reputation damage, and financial loss. What is your reputation worth? If you experienced a data breach like the credit card processor, CardSystems, would you survive? They didn’t. The dollar costs to clean-up after a breach will far exceed the costs to implement proactive security, the financial losses reimbursed to customers, the manpower to recover systems or to issue new card or account numbers, the loss of market share, and the civil monetary penalties for violations of law, not to mention damage to personal reputations.

Your organization may not be a Fortune 500 financial corporation, but you can cost-effectively leverage leading data leak prevention technologies, just as the big financial corporations have, to protect NPI and PII. Citibank and Bank of America have clearly demonstrated that when given a choice, customers choose financial services organizations that put their privacy on the list of critical service requirements. By implementing a marketing strategy that leverages state-of-the-art security practices with strong security branding, your organization can recognize the business benefits of a proactive security program.
An Overview of Customer Data Privacy Regulation In the Financial Services Sector

Mapping Regulatory Requirements for the Protection of PII & NPI to Intrusion’s Security Compliance Products

The following diagram is a useful aid for understanding how Intrusion’s Compliance Commander family of security products can address the regulations discussed in this whitepaper.

**Gram-Leach-Bliley Data Protection Act**
- Protect security, confidentiality, and integrity of PII
- Protect against unauthorized access to, or use of, information
- Assess risks:
  - Identify vulnerabilities and threats
  - Identify and classify information assets
- Assess and mitigate risk:
  - Design and implement security controls
  - Prevent or mitigate potential damage
- Control access to electronic PII
- Secure electronic PII
- Encrypt electronic PII in-transit
- Monitor to detect actual or attempted attacks on, or intrusions into, PII
- Monitor changes in threats or technology

**Identity Theft Act**
- Protect PII from unauthorized access and use
- Monitor and filter electronic information for exposure
- Enable rapid response
- Report suspicious activity

**The USA Patriot Act**
- Verify customer identity
- Monitor information in-transit
- Ensure rapid alerting and response of unauthorized access or disclosure of PII

**Compliance Commander Solutions**

**Sentry**
- Data sensors for identifying, classifying and protecting PII
- Content monitoring and filtering (data leak prevention)
- Dynamic Application Detection™ ensures protection for all ports, protocols, and applications, known or unknown:
  - Email
  - HTTP
  - IM / P2P
  - FTP
  - Telnet
  - File attachments (.doc, .ppt, .xls, .pdf, .txt, many others)
  - All other ports and protocols
  - Identification and blocking of targeted attacks
  - Policy enforcement and management
  - Event logging and alerting
  - Real-time monitoring
  - Rapid response and remediation capabilities
  - Audit trail
  - Scalable and comprehensive reporting

**Database Defender**
- Database and file server activity detection and monitoring
- Database and file server protection:
  - Inspects all data streams
  - Detects illegitimate access or suspicious activity
  - Alerts when new or unknown applications attempt access
  - Alerts when unauthorized devices or clients attempt access
  - Provides forensic and audit capabilities
  - Enables rapid response and remediation
  - Comprehensive reporting capabilities

**Sarbanes-Oxley Act**
- Protect security, confidentiality, and integrity of NPI
- Secure NPI infrastructure
- Monitor IT processes and NPI for unauthorized disclosure, access, abuse, or manipulation
- Implement internal controls
- Ensure rapid reporting and public disclosure of material events

**Basei II**
- Proactive risk management, including policies and procedures to reduce operational risk and protect information assets:
  - Monitoring for violations to mandates and security procedures
  - Reporting of unauthorized disclosure or access to information assets

**NASDAQ 3010 (d)**
- All incoming and outgoing written and electronic correspondence relating to securities business or investment banking must be reviewed
- Procedures must be developed for the review of all incoming and outgoing written and electronic correspondence
- All customer complaints, whether received in email or other electronic or written form, must be reported to the NASD

**CA SB 1386, AB 1950, State Data Protection Laws**
- Protect NPI collected electronically:
  - Implement security controls to protect NPI
  - Monitor for security breaches
  - Utilize encryption of NPI
  - Ensure rapid reporting and disclosure of security breaches

**EU Privacy Directive**
- Protect the security, confidentiality, integrity of NPI (requirements mirror GLBA mandates)

**Payment Card Industry Security Standards**
- Protect security, confidentiality, and integrity of NPI:
  - Encrypt cardholder data
  - Log and monitor electronic communications
Sentry™ is the industry’s leading data leak prevention product which prevents NPI, PII and other database information from leaving your network unprotected. It dynamically protects all ports, protocols, and applications against intentional and unintentional network data leaks. These leaks can originate from business partners, customer support operations, mobile workers, or Trojan / backdoors and other malware designed to capture PII.

Database Defender™ is a database activity detection and monitoring tool that moves security safeguards closest to the database assets themselves, thereby protecting against authorized and unauthorized insider and business partner risks. Database Defender™ is a self learning security application that recognizes abnormal database access activities and stops unauthorized access.

Both Sentry™ and Database Defender™ are managed from Provider™, the unified management console for Intrusion’s Compliance Commander security product portfolio.

Contact us at sales@intrusion.com or call 1(888) 637-7770 for more information and to learn how we can help you mitigate your security risks associated with PII and NPI.

About the Author

Susan Orr is a leading financial services consultant with extensive experience in regulatory, risk management, and security best practices. During her 14 year tenure as a bank examiner, she held numerous lead positions, including: Regional IT Examination Specialist, Special Assistant to the Regional Director, Special Assistant to the Director of DSC, and Special Assistant to the Vice Chairman of the FDIC. Susan was also a lead instructor for the FDIC’s technology school and was instrumental in key industry initiatives, such as the FDIC e-Risk Strategic Initiatives Risk Monitoring Committee, the Chicago Region Interagency Technology Group, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook rewrites.

Prior to launching her consulting practice, Susan was Vice President of Regulatory Compliance for an Internet security company where she advised staff, customers, and partners on regulation, security, and risk management. She retains close relationships within the FFIEC agencies as well as industry trade groups to stay abreast on new technologies, best practices, and regulatory issues. Susan is a Certified Information Systems Auditor (CISA), a Certified Information Security Manager (CISM) and a Certified Risk Professional (CRP).