



I. Inventory and Limit Access to Sensitive Consumer Information

- **Exited select consumer-sensitive data markets not covered by the Fair Credit Reporting Act. Discontinued selling products that contain SPII¹ (e.g., social security and driver's license numbers) in selected markets, at a cost of approximately \$15-\$20 million in revenue.**

- **Changed process for distributing SPII. ChoicePoint no longer distributes information products that contain SPII except:**

- to support consumer initiated transactions such as for insurance, employment and tenant screening, or financial
- to provide authentication or fraud prevention tools to large accredited corporate customers where consumers have or want to establish relationships (e.g., fraud prevention tools for identity verification, customer enrollment and insurance claims)
- to assist federal, state and local governments and criminal justice agencies

Even for these services, SPII and dates of birth may be masked from view, truncated, or echoed (mirrored) back if provided by consumers.

- **Conducted a company-wide inventory of all applications containing PII² or SPII and update inventory on a quarterly basis.**

- **Remove certain non-SPII from tenant screening reports to further reduce potential risk.**

- **Truncate SPII and dates of birth in civil and criminal records returned from public record sources for background screening solutions.**

- **Restrict resellers access to credit data and motor vehicle data (with certain exceptions) in background screening solutions and insurance services.**

- **Established procedures to properly secure appropriate physical media containing SPII while being shipped.**

II. Credential Customers, Employees, and Vendors

- **Established a Corporate Credentialing Center for customer credentialing.**

- **Strengthened customer credentialing procedures utilizing multiple internal and external sources and an expanded site visit program.**

- Recredentialed existing customers regulated by the Fair Credit Reporting Act (FCRA) in 2006 and 2007, requiring:
 - successful completion of credentialing process
 - certifications of permissible purpose
 - site visits (with limited exceptions)
 - quality control review

SPII: ¹ Information owned or licensed by ChoicePoint that consists of an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: (1) driver's license or state identification number; (2) social security number; or (3) account numbers (such as bank, credit or debit card numbers) when combined with any required security code, access code, or password that would permit access to an individual's financial account.

PII: ² Individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name or first initial and last name; (b) a home or other physical address, which includes at least street name and name of city or town; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number with expiration date; (g) date of birth; (h) a driver's license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above.



- Ongoing credentialing of new customers regulated by the FCRA, requiring:
 - successful completion of credentialing process
 - certifications of permissible purpose
 - site visits (with limited exceptions)
 - quality control review
 - Recredentialed existing customers not regulated by the FCRA in 2006 and 2007, requiring:
 - successful completion of credentialing process
 - quality control review
 - Ongoing credentialing of new customers not regulated by the FCRA, requiring:
 - successful completion of credentialing process
 - site visits (with limited exceptions) if receiving untruncated SPID
 - quality control review
- **Implemented employee and independent contractor court researchers (ICCRs) credentialing and recredentialed programs.** Employees and ICCRs located in the U.S. consent to a pre-employment background check and a recredentialed background check every three years.
- **Developed a Third Party Service Provider (TPSP) Program.** Through an assessment process, the TPSP Program helps to ensure that vendors having access to PII and SPID have implemented and maintain appropriate information security and privacy safeguards and are qualified to have access to ChoicePoint information. All eligible TPSPs completed the assessment by the end of 2007 and will be re-assessed annually or semi-annually depending on their risk category.

III. Establish Corporate Accountability

- **Established Office of Privacy, Ethics and Compliance (Formerly Office of Credentialing, Compliance and Privacy).**
 - Headed by the General Counsel and Chief Privacy Officer
 - Office reports to the Privacy and Public Responsibility Committee of the Board of Directors on privacy matters
 - Office is responsible for company-wide privacy, ethics, compliance, and internal security matters.
- **Created corporate-wide accountability for privacy and security.**
 - Security Advisory Committee (senior leadership)
 - Security Working Group (key managers)
 - Credentialing Working Group
 - Policy Working Group
- **Members of the Office of Privacy, Ethics and Compliance obtained International Association of Privacy Professionals Certification.**
- **Members of Information Security obtained Certified Information Security Manager Certification.**
- **Designated privacy and security representatives within each business unit who assist with implementation of security and privacy policies, compliance and privacy matters.**

IV. Execute Policies, Procedures and Guidelines

- **Developed, codified and/or amended more than 90 policies, procedures and guidelines.** Policies focus on the following areas (list is not exhaustive):
 - Data access, protection, transfer, transport, restriction, retention, destruction and classification
 - Information Security Breach Response and Notification
 - Incident Response
 - Credentialing and Recredentialed
 - Physical Security



- Public Representations
- Information Security
- Code of Conduct

V. Self Regulate Through Audit and Compliance

External

- **Underwent a comprehensive independent assessment of our privacy and information security program in 2006 and 2007.**
- **Successfully completed 43 third party audits in 2005; 40 in 2006; 30 in 2007; and 5 to-date in 2008.**

Internal

- **Enhanced internal audit and compliance program.**
 - Engaged outside privacy experts in 2005 to assist in developing privacy compliance framework
 - Increased compliance audit staff in 2005, 2006 and 2008
 - Automated customer and consumer audit processing
 - Implemented plan that incorporated auditing a percentage of new accounts
 - Increased the number of accounts and transactions audited each year since 2005
 - Added additional Business Units/Products to the compliance audit program in 2007
 - Implemented insurance customer audit program
 - Enhanced reseller compliance audit program to include site visits and self assessment questionnaires
 - Expanded reseller compliance audit program to include additional resellers in 2007
 - Increased number of states in which we conduct Motor Vehicle Records (MVR) audits
- **Conducts various audits of:** FCRA customer permissible purpose; consumer sampling verifying FCRA permissible purpose; non-FCRA customer business purpose; customer usage of data; reseller; corporate credentialing center; mandatory training; Web site privacy policies; public representations; regulatory compliance; and ChoicePoint policies.
- **Conducted a corporate-wide review of online Web site privacy policies in 2005 and 2006.** Amended online privacy policies to be more reflective and transparent of the Web site practices. Obtained online privacy seal certifications for consumer-facing sites.

VI. Implement Technology Solutions

- **Implemented an information security control framework. Enhance and test it continuously.** ChoicePoint adopted a widely accepted framework, ISO Standard 27002, and tailored and expanded the framework to ensure appropriate administrative, physical and technical safeguards exist across the business units.
- **Enhanced network security.**
 - Implemented technical standards, patch management and anti-virus standards enterprise-wide
 - Improved vulnerability assessment program
 - Monitor access to critical databases containing SPII
- **Implemented external Web server scans and application scanning services to trap e-mails containing SPII**
- **Initiated a technology implementation to restrict write ability on mobile media devices**
- **Implemented access restrictions to categories of Web-sites deemed malicious or dangerous**
- **Implemented on-going encryption technology.**
 - Implemented various technologies for secure messaging and encryption, to include enabling encryption technology for 20+ business processes, including customer related processes, protection of mobile devices, and database encryption for multiple business units to protect millions of rows of SPII. These include the following types of encryption:

- Transport Layer Security (TLS)
 - Pretty Good Privacy (PGP)
 - Voltage Identity Based Encryption (IBE)
 - Enabled our businesses to be compliant with Payment Card Industry standard using database encryption
 - Encrypted laptop hard drives
- **Developed a data classification tool.** Provides ChoicePoint associates the ability to classify data based on sensitivity.
 - **Upgraded internal Identity Access Management System to streamline user lifecycle management process.**
 - **Perform monthly password assessments.** Internal access team conducts assessments and forces users with weak passwords to change their password upon next login.

VII. Train and Educate Associates

- **Developed and implemented mandatory annual online training programs with assessments.**
 - **Privacy** - focuses on laws, regulations, ChoicePoint Privacy Principles, policies and procedures that govern privacy.
 - **Information Security Awareness** - focuses on the importance of information security, information classification levels, record retention and disposal procedures, social engineering, e-mail and Internet usage guidelines, viruses, passwords, and suspicious activity.
 - **Code of Conduct** - focuses on professional, ethical, legal and socially responsible behavior for ChoicePoint associates.
 - **Record Retention and Deletion Policy** – focuses on record retention, deletion, and legal hold procedures.
- **Distribute privacy reminders to all associates.** Important ChoicePoint privacy and information security policies and practices are reinforced through electronic privacy reminders to associates.
- **Distribute Privacy Principles to associates quarterly.** ChoicePoint Privacy Principles outline how PII and SPII is accessed, transferred, collected, maintained, used or disseminated by ChoicePoint in delivering information products and services through any ChoicePoint company or line of business.

VIII. Enhance Internal and External Outreach Program

- **Conducted 63 outreach events in 2005; 69 in 2006; 79 in 2007; and 35 to-date in 2008.**
- **Instituted program to notify privacy stakeholders of privacy-related announcements.** Notifies stakeholders on key ChoicePoint programs and on privacy and information security enhancements.
- **Established liaison with law enforcement to stay informed of latest identity theft threats.**
- **Partnered with the American National Standards Institute and the Better Business Bureau.** ChoicePoint along with eight other founding partners published Identity Theft Prevention and Identity Management Standards on January 31, 2008. (Full report available at: http://www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3).
- **Established relationship with Identity Theft Resource Center (ITRC).** Partnered with the ITRC to help fund assistance to victims of identity theft.
- **Created hotlines.** A dedicated privacy hotline (877) 301-7097, Whistleblower and Fraud Reporting hotline (866) 473-3728, United Kingdom Fraud Hotline +44 (122) 347-0810, and Australia Hotline (800) 246-12376 were created to give individuals direct access to the appropriate office to ask privacy related questions or to report suspicious activity.



- **Created a dedicated privacy Web site.** www.privacyatchoicepoint.com. Web site was designed to provide information about ChoicePoint's commitment to privacy and security, ChoicePoint's Privacy Principles, and Opt-Out Procedures.
- **Invited to Federal Trade Commission-sponsored workshop in April 2008 to present on "How to Build a Culture of Privacy and Security."**
- **Received third-party recognition of industry-leading privacy and security practices from major media outlets/privacy advocates including:**
 - *New York Times*, November 12, 2006
 - *Inside 1-to-1 Privacy*, December 6, 2006
 - *USA Today*, April 2, 2007
 - *Privacy & Security Law Report*, October 29, 2007

IX. Transparency with Consumers

- **Established Consumer Advocacy Office.** Enhances interactions with consumers in five key areas:
 - Consumer outreach
 - Consumer advocacy
 - Consumer assistance
 - Consumer policy
 - Internal awareness
- **Enabled consumers to request certain information available about them on www.ChoiceTrust.com.** Certain information can be ordered and delivered online for free. The information includes FCRA and FACT Act reports as well as public record searches.
- **Created vehicle for correction.** If any of the information appears to be incorrect to a consumer, individuals have the right to dispute the accuracy of the information in the reports provided by ChoicePoint and may do so by e-mailing consumer.center@choicepoint.com or calling the number listed on their reports.
- **Developed a consumer-oriented video.** Video explains the benefits consumers receive as a result of ChoicePoint's insurance and background screening services. Video available for viewing on www.ChoicePoint.com.