CALIFORNIA'S NEW SECURITY BREACH DISCLOSURE REQUIREMENTS

SCOTT W. PINK
GRAY CARY WARE & FREIDENRICH
spink@graycary.com
(916) 930-3271

ISACA FALL CONFERENCE
September 23, 2003

Gray Cary

- Silicon-Valley Based Law Firm.
- Offices in Bay Area, San Diego, Austin, Seattle, Sacramento and Washington, D.C.
- Represent Fortune 500 and Emerging Growth Technology Companies.
- Intellectual Property and Services.
- Privacy Services.

Cybersecurity Trends

- Cybersecurity threats have existed for some time, but security not a priority for many companies.
- Attacks are continuing and potential damage significant.
  - Compromised, lost or destroyed data.
  - Loss of business.
  - Loss of productivity.
- New potential legal liabilities have emerged.

Legal Background

- Historically, legislation has focused on regulated industries
  - Financial – Gramm Leach Bliley.
  - Health – HIPAA.
- 9/11 raised national security issues:
  - Passage of Patriot Act increased investigative powers of law enforcement for cybersecurity and other threats.
  - Critical Infrastructure Information Protection Act encourages sharing of information with Department of Homeland Security.

Legal Trends

- Increasing interest in consumer protection.
- FTC actions under Section 5 of FTC Act against Eli Lilly, Microsoft and Guess relating to security procedures promised in privacy policies.
- These enforcement actions focus on existing unfair trade practice laws.
- Companies required to implement comprehensive security program with external audits.

Legal Trends

- Public companies may have obligation to implement cybersecurity under Section 404 of the Sarbanes-Oxley Act.
- New SEC Rules: annual internal control report must contain a "statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company."
- “Internal control over financial reporting” = process that provides reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.”
- Private companies thinking of going public may want to bring their systems into compliance.

California's New Security Breach Disclosure Requirements

- SB 1386 – Took effect on July 1, 2003.
- Designed to address identity theft problem.
- Passed over industry opposition.
- Not yet tested in court.
- Creates new disclosure requirements for security breaches for government agencies and businesses.
- Focus on requirements for business.

Who is covered by new law?

- Applies to:
  - Any person or business that conducts business in California and
  - Owns or licenses computerized data that contains personal information or maintains such computerized data for another.
  - Also applies to California state agencies.

What information is covered?

- Personal information:
  - Individual's first name or initial and last name **in combination** with one or more of the following "data elements":
    - Social security number
    - Driver's license number or California ID number
    - Account number, credit or debit card number in combination with required security code, access code or password that would permit access to account
  - Data elements must be **unencrypted**
  - Does not include publicly available information that is lawfully made available from government records

Disclosure Obligations

- Covered businesses must disclose:
  - Any breach of the security of the system following discovery or notification of the breach.
  - Breach = unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of PI of a **California resident**.
  - Good faith acquisition by employee or agent is not breach, provided not used for further unauthorized use or disclosure.

Notice Requirements

- Owners of computerized data must disclose to affected California residents; maintainers of such information must disclose to owners (who in turn must disclose to affected persons).
- Notice must be given to any resident of California whose PI is or is reasonably believed to have been acquired by unauthorized person.
- Notice must be given in "most expedient time possible" and "without unreasonable delay" consistent with:
  - Needs of law enforcement.
  - Necessary measures to determine scope of breach and restore reasonable integrity of system.

Notice Requirements

- **Notice can be provided in the following ways**:
  - Written notice
  - Electronic notice consistent with E-Sign Act.
  - Substitute notice if cost exceeds $250,000 or affected class exceeds 500,000 or do not have sufficient contact information. Must do all of the following
    - Email to those for which it has addresses
    - Conspicuous notice on web site
    - Notice to major statewide media
- **Can follow existing internal procedures if consistent with time requirements of the law**

Remedies for Violations

- Private right of action preserved over industry opposition.
- Cal Civ. Code Section 1798.84 provides for:
  - Damages.
  - Injunctive relief against company that violates, threatens to violate or has violated the requirements.
  - These are cumulative to other remedies that might exist at law.

Unresolved Issues

- Does this violate dormant Commerce Clause?
  - Ferguson v. Friendfinders, Inc., 115 Cal.Rptr.2d 258 (2002) upheld spam law against similar challenge.
- What kind of knowledge triggers disclosure and at what level of the company?
- Is encryption of data elements sufficient to avoid disclosure requirements?
- Does a request by law enforcement not to disclose provide immunity?
- What impact does an erroneous disclosure have?

Compliance

- Review existing systems to evaluate technological issues regarding detection and notice.
- Assess whether Personal Information is encrypted and if not, determine if encryption can be applied.
- Review existing procedures or create new procedures for reporting consistent with SB 1386.
  - Establish levels of detection, response, and notification responsibility within organization.
  - Establish procedures with local law enforcement. Create mechanism for keeping records of the notifications provided
  - Educate and train employees with need to know about the new requirements
- Litigation will influence compliance.

Trends?

- Proposed federal law – Notification of Risk to Personal Data Act (S. 1350)
  - Modeled after California law.
  - Applies to any company engaged in interstate commerce.
  - Anti-fraud and notification procedures under GLB may suffice.
  - Civil penalties, but no private right of action – enforced by FTC or the attorney general of a particular state.
  - Preempts state laws except California's.

THE END

THANK YOU FOR YOUR ATTENTION

About the Speaker

Scott W. Pink is Special Counsel in the Intellectual Property and Transactions Group of Gray Cary Ware & Freidenrich, a national law firm based in Silicon Valley that represents leading technology companies. Before joining Gray Cary, Scott was Vice President, General Counsel and Secretary for Prima Communications, Inc., an international publishing company that was sold to Random House. Scott served on the company's executive committee and was responsible for the contractual and legal affairs of the company. Scott has also been a partner in a major San Francisco law firm and a law clerk to the U.S. Court of Appeals for the Ninth Circuit.

Scott is a recognized expert on internet and cybersecurity law. He is currently deputy chair of the American Bar Association Business Law Section's "Cybersecurity Task Force". He has spoken on cybersecurity and specifically on California's new security breach disclosure requirements to the American Bar Association, the Information Technology Association of America, the SDForum, and many other groups. He has published several articles on the subject, including "The New Cybersecurity Paradigm: California Law Now Requires Disclosure of Security Breaches" published in the June 30, 2003 issue of BNA's Privacy & Security Law Report.

Scott is also an expert in intellectual property law and transactions. He has served as chair of local, state and national intellectual property organizations and has spoken to many organizations on the subject of intellectual property law, licensing, distribution and outsourcing transactions, and strategic alliances. He is the author of many publications, including *The Internet and E-Commerce Legal Handbook* published by a division of Random House, *Protecting Trademarks in Cyberspace*, Cover Story for January 2002 issue of the ACCA Docket, *Electronic Filing of Trademark and Patent Applications*, July/August 2002 issue of the ACCA Docket, *State Spam Laws Survive Constitutional Scrutiny, but Should Congress Enact a Federal Law*, April 2002 Journal of Internet Law, and *Publishing in the Digital Age*, The Transnational Lawyer, Spring 2002. He also served as an adjunct Professor of Law at UC Davis Law School. Scott is a graduate *cum laude* of Harvard Law School and *magna cum laude* of Harvard University, where he was a starter on the lacrosse that finished in the top ten nationally.