

5 Questions...

Volume 1 Issue 3

Fall 2008

5 Questions seeks out experts in their respective fields to answer...well, five questions on topics of importance to securities industry professionals in the field of compliance and regula-

Security Breach Incidents

1) We have seen a plague of breaches over the past several years. What's going on?

Starting with California in 2003 and now across 44 states, laws require companies to notify affected individuals when their unencrypted personal information is accessed or acquired by anyone not authorized for that purpose. Estimates of the number of personal records breached in the USA just since 2005 involve over 200 million records! Alarming, breaches happen due to negligence as often as malice; for those caused by criminal hackers, the breach is most often discovered only months following the actual breach. As more companies gather more information to use for products and services, the frequency of breaches increases.

2) What can companies do to change this rising tide of breaches?

First of all, on the fly compliance, like patching security gaps as they are exposed through breaches, is not sufficient. Firms must anticipate threats and vulnerabilities, train staff to close gaps to lower risk profiles, and prepare response plans for when things do go badly.

3) Why have a response plan if the object is to prevent breaches in the first place?

Realistically, privacy and security breaches will be reported and companies have to be ready to investigate and respond. A good plan details steps to...

Continued on page 2

Our guest: Richard Purcell CEO, Corporate Privacy Group

Underlying the SEC's proposal to significantly broaden Regulation S-P's safeguarding and disposal provisions is concern over the increasing number of information security breaches and the potential for identity theft and other misuse of personal financial information at BDs and RIAs. **Richard Purcell** is a leading voice in addressing consumer privacy and data protection challenges. His firm, **Corporate Privacy Group**, was named one of the Best Privacy Advisers for 2007 by Computerworld Magazine. We are privileged to have him as this edition's special guest...



5 Questions: Security Breaches (cont.)

3) Why have a response plan if the object is to prevent breaches in the first place?

(Continued from previous page) ...determine what happened, what data has been put at risk, who needs to be notified, how to handle the notification itself, and how to resolve the causal factors to prevent further breaches. Notification may include not only the affected individuals, but also law enforcement, shareholder representatives, credit companies, and others. Experience has shown that customer response to notices requires thorough preparation of customer service centers to handle the load and respond to the inquiries with appropriate advice and protections.

4) What kind of data is generally involved in past breaches?

The laws vary, but all focus on information that can be used to identify, contact, or locate an individual person. A study of about 500 breach incidents by Verizon Business Security (<http://www.verizonbusiness.com/resources/security/databreachreport.pdf>) indicates that credit card data is the target of most breaches, involved in 84% of the breaches examined. Even though over 70% of the sources of the breach came from external sources, those perpetrated by internal sources (18%) accounted for 10 times the amount of data.

5) Isn't it better to prevent breaches so I don't have to engage in breach notifications?

Of course, preventing these events is the first priority. The checklist includes several entries:

- Examine all policies and supporting procedures to make sure what you expect to happen is really happening; over half of incidents are caused by significant errors in procedures
- Maintain all systems by constant updates and technical upgrades; breaches caused by exploits of a known vulnerability account for over 20% of incidents
- Collect only that information needed to serve your business purposes and retain that information only as long as it is needed

Richard Purcell, a noted privacy expert, helps Fortune 100 companies and government agencies build strategic and sustainable privacy programs...

- Protect personal information with the same concerns used to protect intellectual property and confidential business data
- Make privacy and security a component of enterprise strategy with appropriate staffing and funding



THE SUTRO GROUP

THE SUTRO GROUP LLC

P.O. Box 29025
San Francisco, CA 94129

Phone: 415-888-8055

Fax: 415-380-7964



THE SUTRO GROUP

We're on the web!
www.thesutrogroup.com

To Our Colleagues:

Compliance professionals are being challenged by one of the most tumultuous periods in the history of the financial markets: the Societe Generale trading scandal, the demise of Bear Stearns and Lehman Bros., continuing fallout from the credit crunch (including the acquisition of Merrill Lynch by B of A and the conversion of Morgan Stanley and Goldman Sachs into Bank Holding Companies), a volatile and uncompromising stock market and very active rule making by the SEC (i.e. restrictions on short selling, forthcoming regs on privacy etc.). In *5 Questions*, we'll highlight important issues and offer practical advice that will help legal and compliance professionals meet the challenges of today's complex regulatory environment. We look forward to working with you...

Best regards,

The Sutro Group & Privacy: News and Notes

[The Sutro Group Can Help](#)

We are currently performing a Privacy Risk Assessment for one of our clients based on the standards set forth in the SEC's proposed revisions to Regulation S-P. As part of this engagement, we are performing an audit of our client's privacy practices, identifying gaps between their privacy practices, written policies and regulatory requirements, and creating privacy WSPs. Combining hundreds of hours of study with years of hands-on experience, The Sutro Group has developed a proprietary system of privacy auditing and risk assessment that is scalable for financial services firms of all sizes. Get ready for the new privacy rules by partnering with The Sutro Group, one of the most trusted names in regulatory compliance. For more information, please contact us by [clicking here...](#)

DISCLAIMER

Materials on this site have been prepared by The Sutro Group for general informational purposes only. These materials do not, and are not intended to, constitute legal advice. The content of this site concerns topics selected by The Sutro Group for dissemination to the general public, and is offered on a blind basis, without any knowledge as to your industry, identity or specific circumstances. The content of this site should not be relied upon or used as a substitute for consultation with professional advisors.