

Developing An Incident Response and Security Breach Notification Plan

Jeffrey P. Weingart
Kristen J. Mathews

December 13, 2005

Brown Raysman Millstein Felder & Steiner LLP

Security Breaches

2005

CSI/FBI COMPUTER CRIME AND SECURITY SURVEY

CSI/FBI Survey

1. Virus attacks continue as source of greatest financial losses. Unauthorized access showed a dramatic cost increase, replacing denial of service as second most significant contributor to computer crime.
2. Web site incidents have increased dramatically.
3. Use of cyberinsurance remains low.
4. Most companies conduct security audits and have security awareness training.
5. Report available at www.gocsi.com

CSI/FBI On Information Sharing

- Organizations still reluctant to report security breach incidents to law enforcement.
- Factors: Negative publicity, advantage to competitors.
- Greater emphasis on civil remedies.
- Lack of understanding of law enforcement interest or involvement in the area.

Data Security Breach Incidents Continue to Make News

TransUnion notifies consumers of data loss

A burglar stole a desktop computer containing sensitive data

News Story by [Jaikumar Vijayan](#)

NOVEMBER 09, 2005

Patients' personal information stolen from UT Medical Center

October 31, 2005

Bank of America notifying customers after laptop theft

Users of Visa Buxx prepaid debit cards affected

News Story by Robert McMillan

OCTOBER 07, 2005

(IDG NEWS SERVICE) - Users of the Bank of America Corp.'s Visa Buxx prepaid debit cards are being warned that they may have had sensitive information compromised after the theft of an unencrypted laptop computer.

In a letters sent to Buxx users and dated Sept. 23, the Charlotte, N.C.-based bank warned that customers may have had their bank account numbers, routing transit numbers, names and credit card numbers compromised by the theft. Visa Buxx was a prepaid credit card for teenagers that the Bank of America stopped se

The laptop, which belonged to an unnamed Ban Diane Wagner, a company spokeswoman. The sending out the letters after a two-week investig

The Star-Ledger

University exposes students to ID theft

Saturday, October 15, 2005

BY KELLY HEYBOER
Star-Ledger Staff

Montclair State University posted the names and Social Security numbers of 9,100 undergraduates on the Internet for nearly four months, exposing the students to identity theft, campus officials said yesterday.

Embarrassed university administrators sent students a letter on Thursday informing them of the computer glitch and urging them to check if their Social Security numbers have been stolen.

"Certainly our hope is we've caught this in time," said Ann Frechette, a Montclair State spokeswoman.

The university's information technology staff discovered the problem last Friday after an undergraduate put his name into the Google Internet search engine. The site listed a link to a file on the Montclair State Web site that contained the student's name, major and Social Security number.

"He just happened to stumble over it. Fortunately, he was quick to alert our IT department," Frechette said.

edical

heft.

r

Data Security Breach Notification

- April 5, 2002 - Computers at a state data center in California, containing information on as many as 265,000 state workers, were illegally accessed. The breach was discovered on May 7, 2002; employees were not notified until May 21, 2002.
- July 1, 2003 -- law requires any state agency, person or business that conducts business in California to disclose any breach in the security of the data of any resident of California whose certain unencrypted personal information has been compromised and acquired, or **reasonably believed** to be acquired, by an unauthorized person. California Civil Code Sec. 1798.29 and 1798.82-1798.84

California Security Breach Notification Act

Privacy@ChoicePoint

> Consumers > Customers > Media > Investors

CONSUMERS

California Substitute Consumer Notice - Fraud Incident

The following is a letter ChoicePoint recently sent to consumers whose personal information may have been exposed to criminals posing as legitimate businesses.

If you are concerned that your personal information may have been subject to unauthorized access by ChoicePoint users, please feel free to call (877) 547-2518. When you call, please be prepared to provide your name and the last four digits of

Privacy@ChoicePoint

> Consumers > Customers > Media > Investors

CONSUMERS

Information for Consumers

Our primary focus remains assisting those consumers whose personal data may have been fraudulently obtained by criminals. We notified all 145,000 potentially affected consumers via the United States Postal Service. Approximately 35,000 of these consumers are California residents and approximately 110,000 are residents of other states.

For Consumers Who Received a Notification From ChoicePoint

The following information is for consumers who received a notification letter from ChoicePoint.

We notified consumers nationwide and have taken other steps to assist potentially affected consumers whom we have identified to date. ChoicePoint has partnered with [Experian](#), one of the three national credit reporting companies, to provide affected consumers with resources that will help them monitor and protect the use of their personal information free of charge to the consumers. These include:

- a dedicated toll-free customer service number and a special web site to respond to inquiries;
- a combined three-bureau credit report;
- one-year credit monitoring service

Additionally, for anyone who suffered actual identity theft from this fraud, ChoicePoint will provide further assistance to help them resolve any issue arising from that identity theft.

We hope these efforts will help those individuals protect their personal data from being used in a criminal manner and that they will mitigate any harm.

- September 2004, ChoicePoint became aware of “suspicious activity” by some small business customers in California and notified law enforcement authorities; a criminal investigation was commenced
- February 2005, ChoicePoint first notified California residents as required by California Security Breach Notification Act
- February 2005, responding to public complaints and inquiries by Attorneys General in other states, ChoicePoint then similarly notified residents of all states of the incident

FORM 10-Q

CHOICEPOINT INC – CPS

Filed: November 08, 2005 (period: September 30, 2005)

ChoicePoint 10-Q lists numerous legal proceedings and lawsuits related to the fraudulent access incident

- Requests and subpoenas by state AGs related to potential consumer law violations
- SEC investigation of possible insider trading
- Federal Trade Commission inquiry into company compliance with federal consumer information security laws
- Consolidated class actions in C.D. Cal. alleging violations of federal Fair Credit Reporting Act and other claims; similar lawsuits in N.D. Ga.
- Shareholders' suits consolidated in N.D. Ga. alleging violation of federal securities laws by issuing false and misleading information concerning the fraudulent access incident
- Purported class action alleging violations of ERISA for acquisition and retention of company stock by profit sharing plan, brought by beneficiaries
- Shareholders' derivative suit, Ga. State court

Security Breach Issues Bottom Line

CHOICEPOINT INC
as of 9-Nov-2005

Splits: ▼



Copyright 2005 Yahoo! Inc.

<http://finance.yahoo.com/>

Security Breach Incidents: U.S. Residents Affected In 2005?

- Privacy Rights Clearinghouse,
www.privacyrights.org
- PCR: More than 51 million Americans had their personal information compromised since February 2005.
- Some of the culprits:
 - Software programs that monitor keystrokes to acquire passwords
 - Phishing
 - Low-tech techniques, including eavesdropping and dumpster diving

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

Posted: April 20, 2005
Updated November 9, 2005

Privacy Rights CLEARINGHOUSE

3100 - 5th Ave., Suite B
San Diego, CA 92103
Voice: (619) 298-3396
Fax: (619) 298-5681

Web: www.privacyrights.org
Contact Us:

www.privacyrights.org/inquiryform.html

Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 9, 2005	TransUnion	Stolen computer	3,623

The States Respond

- Since March 2005, more than 20 states have put in place legal requirements for notifying the public regarding security breaches involving personal information.
- Many of the statutes are modeled on the California law.
- New York Law, as amended: Effective December 8, 2005.

Data Security Breach Notification

- California, Cal. Civ. Code § 1798.82
 - Notification required if unencrypted consumer data is subject to a security breach

Similar laws have since been enacted in numerous states, including New York State, and in New York City

- New York, Gen. Bus. Law New Art. 39-F, Sect. 899-aa et seq. (enacted Feb. 9, 2005, amended Aug. 9, 2005, effective December 8, 2005)
 - Generally tracks California law
 - Applies to any person or business that conducts business in New York state, but disclosure of breach required only to New York residents
- New York City Int. No. 141-A (May 2005), effective Sept. 16, 2005; preempted by New York State law on Dec. 8, 2005
 - Applies to businesses required to be licensed by NYC Dept. of Consumer Affairs

Data Security Breach Notification

California:

Personal Information: Information that triggers the notification requirement -- combination of:

- (A) an individual’s first name (or first initial) and last name, in combination with:
- (B) any of the following data elements: (1) a social security number, (2) driver’s license number or California Identification Card number, or (3) account number, credit or debit card number, together with access code that permits access to “financial account”
- * Safe Harbor: Either (A) or (B) is “encrypted”

Data Security Breach Notification

California:

Notification Requirement - Breach of Security of the System:

- unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of “personal information” maintained by a business
- to California residents whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person

Data Security Breach Notification

New York:

Private Information: Information that triggers the notification requirement -- combination of:

- (A) any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person (“Personal Information”) in combination with:
- (B) any of the following elements: (1) a social security number, (2) driver’s license number or Non-Driver Identification Card number, or (3) account number, credit or debit card number, together with access code that permits access to “financial account”

* Safe Harbor: Either (A) or (B) is “encrypted” unless encryption key is acquired as well

Data Security Breach Notification

New York:

Notification Requirement - Breach of Security of the System:

- unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of “personal information” maintained by a business
- to New York residents whose private information was, or is reasonably believed to have been, acquired by an unauthorized person

Data Security Breach Notification

Both California and New York:

- Outsourcing companies obligated to notify owners or licensees of compromises to personal information, who in turn are required to notify affected residents.
- Notification must be made in the most expedient time possible and without unreasonable delay following discovery and preventative or restorative measures, consistent with the legitimate needs of law enforcement, by one of the following methods:

Notice Methods

- Written notice
- Electronic notice
 - **California:** if the notice provided is consistent with the provisions regarding electronic records and signatures. (See 15 U.S.C. 7001)
 - **New York:** if the person to whom notice is being given has consented, and
 - a log is kept of each such notification; and
 - consent to such e-mail notice may not be made a condition of establishing any business relationship or engaging in any transaction
- Substitute notice

Email, posting on business's website and notifying major media (**all three are required**) where a business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the business does not have sufficient contact information.

New York: criteria must be demonstrated to the Attorney General

Notice Methods

- New York: Telephone (provided a log is kept of each notification)
- New York:
 - Notice of a breach must also be given to specified state law enforcement authorities. N.Y. Gen. Bus. Law § 899-aa(8)(a).
 - Notice must also be given to national consumer reporting agencies if more than 5,000 individuals are affected in a single incident. N.Y. Gen. Bus. Law § 899-aa(8)(b)
- California:
 - Existing notification procedures (with consistent timing) as part of Information Security Policy

Data Security Breach Notification

- Remedies
 - California
 - May be enforced through a civil action to recover damages or injunctive relief
 - Class actions not prohibited
 - May be joined by other claims (e.g., unfair business practice, violation of privacy policy)
 - New York
 - May be enforced by an action brought by the Attorney General
 - However, the remedies shall be in addition to any other lawful remedy available

Other State Data Security Breach Notification Laws

- Most are similar to California, but there are significant differences in provisions in individual state laws, even those that generally follow the California model
 - Watch the fine print!
- Current count
 - Over 20 state enactments in 2005
 - Legislation is pending in numerous other states
- Compliance is a moving target

Pending Federal Legislation

- Numerous pending federal bills
- Bills in both Senate and House that would impose a significantly less stringent standard for notification, and would preempt state laws, have progressed significantly in the last month
- Other aspects of State Laws/Related State Laws might survive

Pending Federal Legislation

- The current state of play:
 - S.1326, sponsored by Sessions, ready for floor vote in Senate
 - A bill to require agencies and persons in possession of computerized data containing sensitive personal information, to disclose security breaches where such breach poses a significant risk of identity theft.
 - H.R. 4127, Data Accountability and Trust Act (DATA), sponsored by Stearns, approved by subcommittee
 - Defines a data breach as the unauthorized acquisition of personal information that establishes a "reasonable basis" to conclude that there is a "significant risk" of identity theft
 - Effective Date – One Year from Enactment

Pending Federal Legislation

- Also still pending
 - S. 1332, the “Personal Data Privacy and Security Act of 2005,” sponsored by Specter, ready for floor vote in Senate
 - No notice to individuals required if
 - Risk assessment conducted with federal and state law enforcement authorities concluded that “there is a de minimis risk of harm to the individuals whose sensitive personally identifiable information was at issue in the security breach”; or
 - Three part test is met:
 - » (1) nature of the information is such that it “cannot be used to facilitate transactions or facilitate identity theft to further transactions with another business entity”
 - » (2) the business entity “utilizes a security program reasonably designed to block” fraudulent transactions; and
 - » (3) the business entity has in place a plan to notify individuals if actual fraudulent transactions occur.



Attorney General Petro Sues DSW Over Customer Data Theft

Ohio's is First State Action against Shoe Retailer

June 6, 2005

COLUMBUS - Attorney General Jim Petro today asked a court to order Ohio-based shoe retailer Designer Shoe Warehouse (DSW, INC.) to individually notify each customer whose personal information may have been stolen recently from DSW computer files. Ohio is the first state to sue the retailer over one of the biggest security breaches of its kind in the nation.

"DSW has acknowledged that a security breach led to the loss of more than one million customers' checking and credit information, yet the company has not individually notified each customer to warn them about this mishap," Petro said. "As we have said repeatedly, we see no reason why DSW, working with the credit card companies and the underlying issuing banks, cannot arrange for direct notification of every affected consumer."

He said the consumers should be put on notice to more carefully review their accounts and take steps to ensure the safety of their accounts and personal information. As part of a lawsuit he filed against the company today in Franklin County Common Pleas Court, Petro asked the court to order DSW to directly notify in writing approximately 700,000 customers affected by the security breach and to find that the company's failure to do so is a violation of Ohio's Consumer Sales Practices Act.

DSW, based in Columbus with retail stores in more than 30 states, including Ohio, reported in early March that computer files containing customers' personal information it retained from consumer transactions from mid-November 2004 to mid-February of this year had been stolen. The news prompted responses from Petro admonishing the company to notify all affected customers. (See Ohio Attorney General's Office press releases for [March 10, 2005](#) and [April 22, 2005](#))

The stolen data included DSW customers' names, credit card numbers, debit card numbers, checking account numbers, and driver's license numbers – information the customers had provided to the company in the course of nearly 1.5 million transactions at 108 stores in Ohio

Ohio AG asks court to order DSW to notify customers of data breach.

Ohio's Consumer Sales Practices Act

State Laws - Points of Variance Data

- Activities Covered:
 - Notice, protect and destroy, credit freeze, etc.
- Effect of encryption/redaction
 - “Encryption” not usually defined, but there are a few exceptions
 - “Encryption” - “the disguising of data using generally accepted practices.” (Maine)
 - “Encryption or by any other method or technology that renders the electronic files, media or data bases unreadable or unusable.” (North Dakota)
 - Several enactments refer to “encryption or redaction”
 - (Arkansas, Louisiana and Illinois)
 - Remedies: Vary

State Laws - Points of Variance

- “No harm, no notice” standard?
 - Notification not required following “reasonable investigation” and determination of “no reasonable likelihood of harm to customers.” (Ark, La.)
 - Notification not required if harm not likely to result, after “consultation with relevant federal, state and local agencies responsible for law enforcement.” (Conn)
 - No harm determination must be in writing and be maintained for five years. (Fla).

State Laws - Points of Variance

- “No harm, no notice” standard?
 - No notification of “technical breach” of system security that “does not seem reasonably likely to subject customers to a risk of criminal activity.”(Wash.).
 - Breach defined as unauthorized acquisition “that materially compromises the security, confidentiality, or integrity of personal information” and “is reasonably believed to cause loss or injury to a Montana resident. (Montana)
 - *The “no harm, no notice” standard been picked up in pending federal legislation*

Top News Article | Reuters.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

REUTERS

Microsoft Red Hat SAIC SBC Communications Sun Microsystems Sybase

Dice™
Look to the tech leader first

Great companies. Great

Change Edition Quote GO symbol lookup Search News GO

Jump To
Channel: YOU ARE HERE: [Home](#) > [News](#) > [Top News](#) > [Article](#)

Fears over identity theft overblown: US study

Thu Dec 8, 2005 11:49 AM ET

[Printer Friendly](#) | [Email Article](#) | [Reprints](#) | [RSS](#) [XML](#)



CHICAGO (Reuters) - A new study suggests consumers whose credit cards are lost or stolen or whose personal information is accidentally compromised face little risk of becoming victims of identity theft.

The analysis, released late on Wednesday, also found that the most dangerous data breaches -- where thieves access social security numbers and other sensitive information on consumers they have deliberately targeted -- only about 1 in 1,000 victims had their identities stolen.

ID Analytics, the San Diego, California-based fraud detection company that performed the analysis, said it looked at four recent data breaches involving a total of 500,000 consumers. It declined to provide the names of the

“New study suggests consumers whose credit cards are lost or stolen or whose personal information is accidentally compromised face little risk of becoming victims of identity theft.”

“...even in the most dangerous data breaches -- where thieves access social security numbers and other sensitive information on consumers they have deliberately targeted -- only about 1 in 1,000 victims had their identities stolen.”

State Laws - Points of Variance Data

- Notification to public agencies and other parties
 - Written notice of the “nature and circumstances” of a security breach must be given to consumer protection authorities. Del. Code Ann. Title 6 § 12B-102(d).
 - Notification must be given to national consumer reporting agencies if more than a specified number of individuals are affected in a single incident:
 - Minn. Stat. § 325E.61(2) (more than 500 persons, notification within 48 hours)
 - Nev. ch. 485 § 24(6) (more than 1,000 persons)
 - N.Y. Gen. Bus. Law § 899-aa(8)(b) (more than 5,000 residents)
 - Tex. Bus. & Com. Code § 48.103(h) (more than 10,000 persons)

State Laws - Points of Variance Data

- Manner of notice/substitute notice
 - Telephone notice permitted
 - Conn. Pub. Acts 05-148 § 3(e)
 - Logs must be kept of electronic and telephone notices. N.Y. Gen. Bus. Law § 899-aa(5).
 - First class mail required
 - Written notification must be given by first-class mail. Me. Rev. Stat. Ann. tit. 10 § 1348(5)(A).
- California substitute notice requires substitute notice be given by all three means of communication (e-mail *and* Web site notice *and* communication with the media).
 - Maine and Texas – e-mail, Web site, media notice are *alternative* means of substitute notice.
 - Me. Rev. Stat. tit. 10 § 1347(7) (e-mail notice, Web site notice *or* communication with the media constitutes substitute notice)
 - Texas Bus. & Com. Code § 48.103(f) (e-mail *or* web site posting *or* communication with the media)

SIIA Calls for Security-Breach Notification Standard - Security Feed - Blog - CSO Magazine - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

CSO The Resource for Security Executives

csonline.com

Search CSO

Search Help

Home

Search

What Is a CSO?

About Us

Magazine

Current

Previous

Print Links

Subscribe/Renew

Newsletters

CSO Conference

CSO Executive Council

Online Features

Alarmed

Analyst Reports

Events Calendar

Metrics

Politics & Policy

Poll

Home > CSO Blogs

Security Feed

Current events and what they mean to your business

Nov 14, 2005

SIIA Calls for Security-Breach Notification Standard

Add Comment (0) | [Permalink](#)

The Software & Information Industry Association (SIIA), a leading industry group, is renewing its call for a national security-breach notification law to replace the slew of state laws that companies are currently reeling with.

Such a law would require the U.S. Congress to establish a "model law for breach notification" to avoid the problem of overnotification, said the SIIA's general counsel and senior vice president, said Wednesday in testimony before the House Subcommittee on Financial Institutions and Consumer Credit.

Bohannon was testifying in connection with a bipartisan proposal called the Financial Data Protection Act or H.R. 3997, which is now before the House Financial Services Committee. The proposed bill was introduced last month and is designed to help consumers by requiring companies that handle their personal information to take steps to protect that data and to notify them in the case of

Industry calls for Security Breach Notification Standard

European Commission

- May follow U.S. lead
- Considering adding security breach notification provision to EU data protection regime

What should you do?

- Audit data collection practices
 - Understand Your Data Flow
 - Try to maintain the Attorney-Client Privilege During Audit!
 - Internal
 - Outsourced
- Encrypt all data
 - Is there true protection against an “inside job?”

Employees the biggest threat to network security

Two vendors debate whether company insiders are a greater security threat than hackers.

By Joseph Ansanelli
Network World, 02/21/05

Today, insiders represent the single biggest security threat for the simple reason that we haven't addressed the problem. That's because IT designed to prevent intrusion from the outside cannot handle the task of keeping confidential data inside the organization. Yet according to Gartner, 84% of high-cost security incidents occur when insiders send confidential data outside the company.

- New York: Encryption key must be secure

Data Security Breach Notification Applications

- Is the answer as simple as “Encrypt Everything?”
 - Hacking into a network/database?
 - Exposure to information on screen?
 - Rogue employee?
 - Stolen printout? Stolen laptop?
 - Stolen/lost PDAs?

What should you do?

- Implement improved internal data handling practices
- Review third-party relationships – operationally and contractually
 - Amend third party agreements as appropriate
 - Check the compliance with law section!
 - What security requirements are included?
 - Indemnification issues?

What should you do?

- Implement an internal information security policy that addresses internal evaluation of security breaches and internal escalation procedures
 - Roll-out and train all employees

What should you do?

- Develop external information security policy that provides for reasonable means of notification of breaches of security.
 - Include appropriate consents to receive notice by e-mail
 - Add to privacy policies, terms and conditions etc.
 - Be careful when amending privacy policies!

Make Your Breach Notices Helpful

Boeing advises ways to foil identity theft - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.grandforks.com/mld/grandforks/business/industries/aviation/13228

GrandForksHerald.com

Posted on Tue, Nov. 22, 2005

Boeing advises ways to foil identity theft

BY MOLLY MCMILLIN
The Wichita Eagle

Boeing is advising current and former employees on steps they should take to prevent possible identity theft after a Boeing computer containing employees' personal information was stolen recently,

The computer held personal information on about 161,000 current and former Boeing employees. It was stolen from a non-B site.

Information on the computer included names, Social Security numbers and, in some cases, bank routing numbers, bank account numbers and home addresses. It did not contain credit card or account passwords.

In an e-mail that most Spirit AeroSystem employees received Monday, Boeing said it wanted to alert workers to the possibility of attempted identify theft or "bank account manipulation." Spirit operates Boeing's former commercial facility.

Former Boeing employees who are affected will receive a letter at home.

Boeing is working with credit reporting agencies Equifax, Experian and TransUnion to provide credit monitoring services. It recommends employees contact one of the three agencies to alert them of the incident and to place a fraud alert on their credit reports.

The initial alert will remain on the credit reports for 90 days, the e-mail said. It will let creditors know to contact the employee before they open new accounts in the employee's name.

The alert lets businesses know that the employees' personal information may have been compromised and requires them to verify identities before issuing credit.

Done

“Boeing is advising ... employees on steps they should take to prevent possible identity theft after a Boeing computer containing employees' personal information was stolen...”

“Boeing is working with credit reporting agencies ... to provide credit monitoring services. It recommends employees contact one of the three agencies to alert them of the incident and to place a fraud alert on their credit reports.”

Have An Incident Response Plan

- Have a Chief Privacy Officer
- Have a list of incident response “team members,” including home contact information
 - CPO, plus representative from IT, PR, HR (if applicable) and legal
- Have single designated contact point to communicate with various constituencies: employees, customers, government, media
- Be prepared to deal with the media:
 - Have list of friendly media contacts in advance
 - Assure media that:
 - preventative personnel and systems are in place
 - investigation is underway
 - situation leading to the breach is remedied or being remedied
 - top-down review of personnel and systems is underway
- Respond Quickly

Contact Information

- Jeffrey P. Weingart
 - (212) 895-2050

Jweingart@brownraysman.com

Kristen J. Mathews

(212) 895-2327

Kmathews@brownraysman.com