FOLEY HOAG LLP

Kroll

Data Breach Prevention and Response

Avoiding Potential Pitfalls and Implementing Best Practices to Protect Your Company

October 17, 2014

Agenda

- Overview of data breach landscape
- Data breach response
  - Technical best practices
  - Legal best practices
- Data breach prevention
  - Technical best practices
  - Legal best practices

Overview of Data Breach Landscape

Alan Brill

A Busy and Dangerous Year

- Attacks continued at a high level
- Cyber-espionage is understood to be an established tool, but hard to determine real volumes, since if you do it right, no one knows you've done it!
- *A high percentage of the attacks were ultimately preventable*
- While some attacks are very high tech, low tech attacks are very popular and often successful
- Perpetrators know this and exploit human weaknesses

Regulators and Litigators Are Noticing Cyber-Security Issues

- FTC, SEC, DHS, HHS and other regulators are recognizing the centrality of cyber and information security to the integrity of our financial infrastructure, and that executives may be held personally responsible
- Companies are receiving significant penalties from the FTC for cyber-security incidents (fines + 20 year audit requirement)
- Boards of Directors are recognizing their responsibility and asking more difficult questions to CEOs and CIOs
- Some companies are considering a “cyber-seat” on the Board, or specialized board advisors
- M&A requires a cyber-security assessment of companies for potential investments

Who are the “bad guys” who commit attacks?

- Today, we find a range of people involved in the cyber-crime/cyber-espionage ecosystem
- Some of the major classifications are:
  - Ideological Attackers
  - Financially Motivated Attackers
  - Cyber-Espionage
  - Cyber-Terrorists

Ideological Attackers (Hactivists)

- Objective is more likely compromise of the entire platform to use or to embarrass (e.g. with a DDoS attack) rather than digging for sensitive data
- BUT, we also see false-flagged hactivist attacks as a “cover” to keep companies busy while the criminals perform other attacks, like installation of malware, with less chance of being noticed!

Financially Motivated Attackers

- Phishing and other forms of credential theft
- Exploit vulnerabilities like SQL Injection, XSS, remote file inclusion
- Increasing use of Ransomware
- Seek intellectual property, trade secrets, plans and other assets that can be turned into money
- They are highly organized, and keep up with the latest technology (for example, exploiting unpatched security holes)

Cyber-Espionage

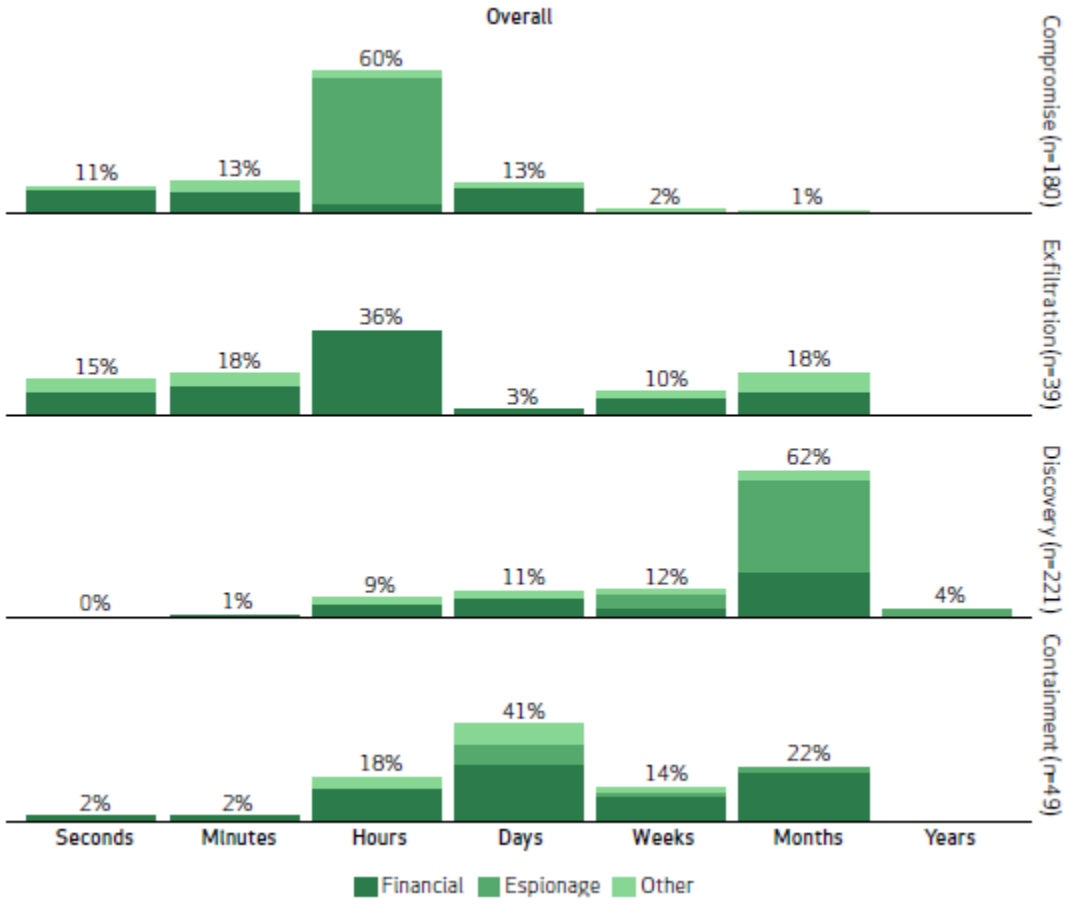
- Second most common cause of confirmed data breaches in 2013 (22%)
- We see that this activity is increasing as the capabilities of this form of asymmetric warfare are achieved by more nations, and more terrorist groups
- The problem is whether our defensive awareness is growing as fast as the abilities of the attackers

Cyber-Terrorists

- They use Cyberspace for many things…
  - Recruiting
  - Publicity
  - Communication and Coordination
  - Offensive/Defensive Cyber Operations

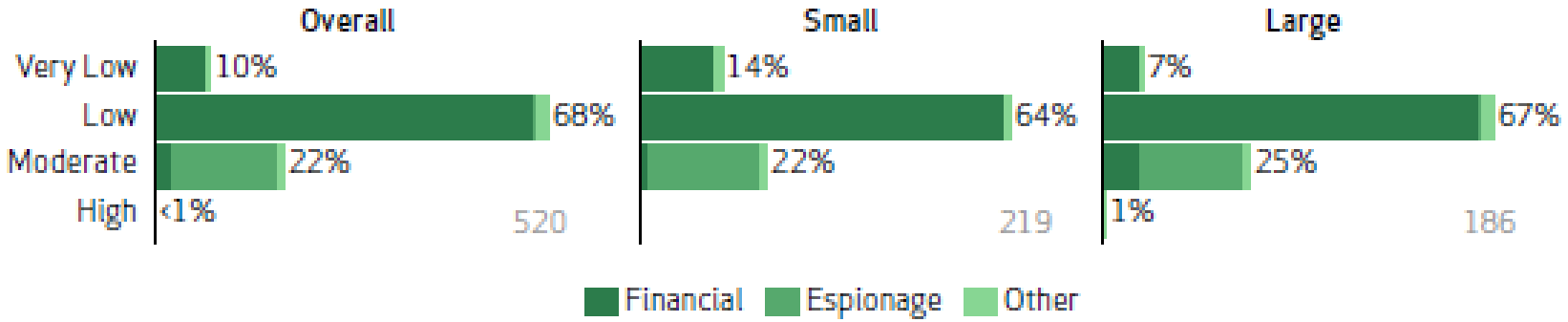
Difficulty of Detection

- Discovery takes a LONG time
  - 62% of the time, incidents not discovered for MONTHS after the actual compromise
  - Unfortunately, the time needed to infect and begin extracting information is measured in minutes or hours….

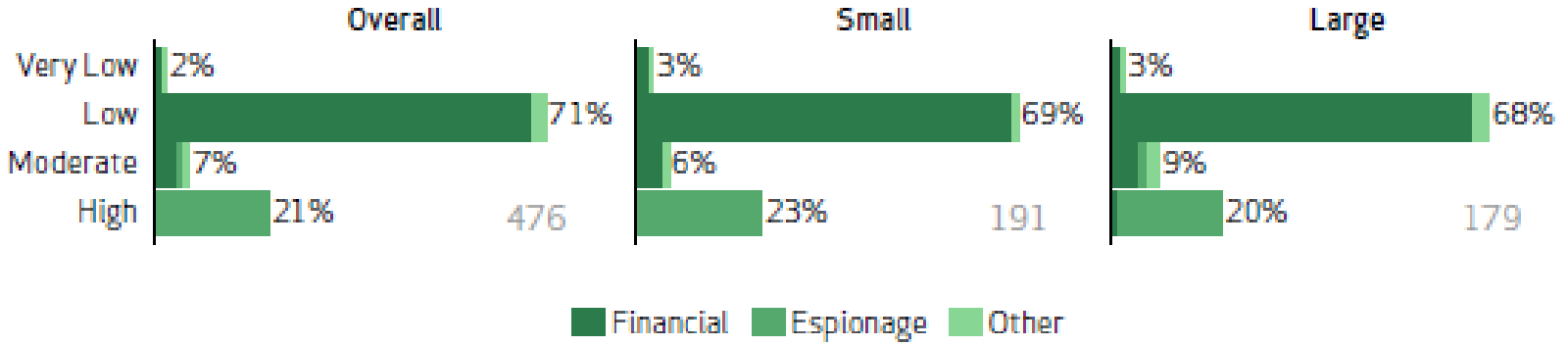


Ease of Compromise

INITIAL PENETRATION OF NETWORK



DIFFICULTY OF SUBSEQUENT ACTIONS



Recognizing Incidents

- While some organizations are improving visibility into their networks through monitoring, many are not
- There is only a slight improvement in the speed of organizations detecting a breach, but attackers are improving their techniques and have the ability to compromise systems faster and to exploit system architecture weaknesses more effectively than ever

The Leakiest Industries

- Finance (465 breaches)
- Government (175 breaches)
- Retail (148 breaches)
- Hotels (137 breaches)

Note that private sector key infrastructure (water, power, etc.) did not make the top 4. This does not mean they are safe from attack!

Data Breach Response

Technical

Alan Brill

Keys to Successful Cyber-Response

- Have resources pre-identified and pre-contracted. You don't have time to deal with contracting delays
- Time is ticking down on state/federal notification deadlines
- Train IT people on how to preserve key logs and other pieces of evidence. Have them forensically collected, perhaps by specialists
- Counsel should check to see if state statutes require computer forensic professionals to hold valid Private Investigator licenses
- You need to determine if an incident occurred, when it occurred, how it occurred, if insiders were involved, and whether the intrusion has been definitively stopped

Keys to Successful Cyber-Response

- Check with your insurer for resources (like forensic specialists) who are on their pre-approved panel
- You may have to use monitoring of the network to independently determine if the incident has stopped
- Cyber forensic investigations can take time, but good practitioners know that you have deadlines and will work to provide the best advice within the schedules of the response team
- One issue that we see is failure to escalate quickly, causing ineffective response and wasted time

Data Breach Response

Legal

Chris Hart

The Costs of a Breach

- Average Date Breach Costs*
  - 2014: $5.9 million ($201 per record)
  - 9% rise over 2013
  - Still lower than 2011 peak ($7.24 million)
  - Companies in healthcare, transportation, and education have the highest average costs, followed by companies in the financial and energy industries.
- And, lost business costs
  - $3.2 million
  - Loss of customers
  - Goodwill, reputation
- Some influences on those costs
  - Presence of a response plan
  - Business continuity management
  - Notification

* *Source: Ponemon Institute/IBM 2014 Cost of Data Breach Study: U.S.*

Some Breaches in the News

- Target
  - 2013 holiday season
  - Over 100 million customers' data compromised (original estimate – 40 million)
  - Estimated cost through the summer: $148 million (Source: Forbes.com, Aug. 5, 2014)
    - $0.11 cost per share
  - Class Action – MDL (Minnesota), consolidating cases in 18 states
- Home Depot
  - Early September
  - 56 million payment cards
  - By Sept. 18 had already cost $62 million
    - Credit monitoring, call center staffing, legal and consulting support
    - Has not yet incurred total losses to reimburse bank fraud, card replacement.
  - 21 federal class action lawsuits as of Oct. 10
- JP Morgan
  - 76 Million households, 7 million small businesses
  - 8-K statement

Incident Response and Investigation

- What is in-house and outside counsel's role in responding to a breach?
- Notice:
  - To federal/state agencies
  - To those impacted by the breach as both a matter of state law and risk management
- Mitigation
- The role of notice and credit monitoring
- In post-breach public statements, what key points should be included to minimize litigation risk?
- To what extent can a company be liable for lost data?

Legal Framework for Breach Response

- **Customer Privacy Laws**
  - Federal and state identity theft laws and regulations
    - Requiring customer notice
    - Requiring information security programs
  - HIPAA / Medical information regulation
  - Gramm Leach Bliley / Financial information regulation
  - Regulations for specific industries (e.g., FCC CPNI Regulations)
  - Laws governing specific information (e.g., Social Security number statutes)
  - Negligence / Consumer protection laws
- **Authorized Use Statutes**
  - Computer Fraud & Abuse Act (CFAA)
  - Electronic Communications Privacy Act (ECPA)
  - Stored Communications Act (SCA)
- **Surveillance / Information Security Law**
  - Federal & State Wiretapping Statutes
  - Invasion of Privacy
- **Property Law**
  - Larceny / Conversion
  - Trade Secrets
  - Copyright / Digital Millennium Copyright Act (DMCA)

Patchwork of Laws

- **Federal laws**
  - "Sector Specific," not comprehensive
  - Two examples
  - Financial Sector
    - GBLA
  - Health Sector
    - HIPAA
- **State Laws**
  - Where most of the action is
  - Some differences
    - How protected information is defined
    - What notification is required
  - Some similarities
    - Cooperation with law enforcement
    - Focus on internal policies

State Law Notification Matrix

STATE	TRIGGER	EXCEPTION	PARTY	PRIVATE ROA?
CA	Acquisition	Lack of Harm	Individuals, CRA	No
FL	Acquisition	Lack of Harm, Consultation with law enforcement	Individuals, CRA	No
MA	Acquisition, Misuse, Risk of Fraud	None	Individual, Owner, AG, other agencies	No
NY	Acquisition	None	Individual, Owner, AG, other agencies, CRA	No
TX	Acquisition	Alternative notification	Individual, Owner, CRA	No

Examples of Notice

Target Breach Notification:

Important Notice: unauthorized access to payment card data in U.S. stores

December 19, 2013

Dear Guest,

We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.

We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV.

We are partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures we can take that would be designed to help prevent incidents of this kind in the future. Additionally, Target alerted authorities and financial institutions immediately after we discovered and confirmed the unauthorized access, and we are putting our full resources behind these efforts.

We recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your credit and debit information. You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 6790
www.equifax.com	www.experian.com	Fullerton, CA 92834-6790
		www.transunion.com

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Again, we want to stress that we regret any inconvenience or concern this incident may cause you. Be assured that we place a top priority on protecting the security of our guests' personal information. Please do not hesitate to contact us at 866-852-8680 or visit Target's website if you have any questions or concerns. If you used a non-Target credit or debit card at Target between Nov. 27 and Dec. 15, and have questions or concerns about activity on your card, please contact the issuing bank by calling the number on the back of your card.

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Examples of Notice

Target Breach Notification (cont.):

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission	Office of the Attorney General
Consumer Response Center	Consumer Protection Division
600 Pennsylvania Avenue, NW	200 St. Paul Place
Washington, DC 20580	Baltimore, MD 21202
(877) IDTHEFT (438-4338)	(888) 743-0023
http://www.ftc.gov/idtheft/	www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission	North Carolina Department of Justice
Consumer Response Center	Attorney General Roy Cooper
600 Pennsylvania Avenue, NW	9001 Mail Service Center
Washington, DC 20580	Raleigh, NC 27699-9001
(877) IDTHEFT (438-4338)	(877) 566-7226
www.consumer.gov/idtheft	http://www.ncdoj.com

IF YOU ARE A MASSACHUSETTS RESIDENT: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address (*e.g.*, a current utility bill or telephone bill);
6. A legible photocopy of a government issued identification card (*e.g.*, state driver's license or ID card or military identification);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time

To remove the security freeze, you must send a written request to each of the three credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Examples of Notice

Sample from Massachusetts AG website:

SAMPLE LETTER TO AFFECTED MASSACHUSETTS RESIDENTS

Date

Consumer Name
Address
City, MA

Dear _____:

We are writing to notify you that a [breach of security/unauthorized acquisition or use] of your personal information occurred on [date(s)].

YOUR NOTICE MUST INCLUDE THE FOLLOWING INFORMATION:

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

[NOTE: Although not required by M.G.L. c. 93H, you should also consider providing the affected Massachusetts residents with additional information to protect themselves against identity theft or other fraud including, but not limited to: the placement of fraud alerts on their credit file; the need to review their credit reports for unexplained activity; and the need to review credit card or other financial accounts for any suspicious and/or unauthorized activity. Many companies provide affected Massachusetts residents with free credit monitoring services. If you are providing credit monitoring services for affected Massachusetts residents, you should provide them with information concerning how they may enroll for such credit monitoring services as well as any telephone numbers or websites that you have set up to answer any questions they may have concerning the incident. Please note that any additional advice provided to affected Massachusetts residents may vary on a case-by-case basis and these information suggestions are not a complete list of all the information that you may want to provide affected Massachusetts residents to better protect themselves against identity theft or fraud].

If you should have any further questions, please contact [provide contact information].

Sincerely,

Protected Information

- This varies from state to state
  - CA:
    - SSN, driver's license, financial account numbers, medical information
  - FL:
    - SSN, driver's license, financial account numbers
  - MA:
    - SSN, driver's license, financial account numbers
  - NY:
    - SSN, driver's license, financial account numbers, passwords, mother's maiden name
  - TX:
    - SSN, driver's license, financial account numbers, medical information, health insurance, passwords, mother's maiden name, date of birth, electronic ID numbers

M.G.L. 93H

- "Personal information" a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:
  - (a) Social Security number;
  - (b) driver's license number or state-issued identification card number; or
  - (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public

Cal. Civ. Code s. 1798.29

(g) For purposes of this section, "personal information" means 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 the data elements are not encrypted:

(1) Social security number

(2) Driver's license number or California identification card number

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

(4) Medical information

(5) Health insurance information

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records

(NB: As Amended by AB No. 1149)

FTC Enforcement

- FTC can bring, and has brought, enforcement actions
  - Has brought actions when it believes that a company failed to have in place adequate security measures
- *FTC v. Wyndham* (DNJ, 2014)
  - Court permitted enforcement action arising out of data breach to proceed under FTC general enforcement powers (Section 5)
  - Suggests broad enforcement authority for FTC based on data breaches, not found in four corners of a statute or regulation

Following Internal Policies

- Element of State and Federal Laws
- Should offer protection consistent with laws in states where they do business
- Companies will be held to their policies
- Balance costs and benefits

Data Breach Response

Panel Discussion and Q&A

Data Breach Prevention Technical

Alan Brill

Top Threats

- Manage ALL “insiders” access –
  limit by amount and time of access, remove when not needed
- Understand network convergence
  - Voice, video, data go over the same networks and share vulnerabilities
- Don’t forget voicemail and conference call hacking

Keys to An Action Plan

- We need to follow the principle **of defense in depth**
- Ultimately, our perimeter defenses WILL fail

–DETER, DEFEND, DETECT, DECONTAMINATE

- We need to better architect our systems to contain outbreaks.
- We need to use basic hardening of all devices
- We need to recognize the need to limit what executes on key servers/machines – white-listing

Keys to An Action Plan

- We need to focus more on monitoring to gain early detection
- Our detection systems need to be tuned to provide actionable intelligence as opposed to millions of warnings
- We need to test the security of our systems regularly – independent testing, both internal and external
- We need this doctrine across government and sensitive infrastructure
- We need to limit users (in-house and external) on a need-to-access basis
- And we need to recognize the evolving definition of “system users”

Data Breach Prevention

Legal

Steve Bychowski

Laws Impacting Data Privacy and Security

- Patchwork of Federal and State Laws Governing:
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
- And then there are the international laws . . .

Basic Template for Federal And State Privacy Laws

- Define the type of “non-public personal information” (“NPI”) that is being regulated
- Provide that NPI must be protected from disclosure to unauthorized holders unless “anonymized” or “aggregated”
- Requires the development, implementation, maintenance, and monitoring of comprehensive, written information security policy:
  - Collect only needed information
  - Retain only as long as necessary
  - Provide access only to those with a legitimate business purpose
  - Implement specific administrative, physical, and electronic security measures to ensure protection
- Requires the disposal of personal information in such a way that it cannot be read or reconstructed

For example, the Massachusetts Data Security Law

Key Requirements:

- Develop a written information security policy
- Designate an individual who will be responsible for your information security program
- Identify what personal information your business possesses, where it is kept and who has access to it
- Place reasonable restrictions on access to personal information: physical restrictions for hard copy files; log-in and password protection for electronic files
- Take steps to ensure that third party service providers have the capacity to protect personal information
- Prevent terminated employees from accessing personal information
- Regular monitoring and updating of security measures

Inventory/Audit

- What Information Do We Have?
- Where Is It?
- Who Has It?
- Why Do They Have It?
  - Why Do We Have It?
- What Are The Risks?
  - How Would Customers and Employees React to Accidental Disclosure?
- What Safeguards Address Them?
  - Physical
  - Technical
  - Administrative
- What Are Our Obligations?

Policies and Procedures: Information Gathering

- Gather no more personal information than is needed
- Remove or block out unnecessary information
- Document any new purposes for personal information
- Conduct regular reviews

Policies and Procedures: Information Security

- Physical, technical, and administrative safeguards
- Safeguards tailored to sensitivity of the information
- Pruning / disposal
- Remember departing employees
- Training

Policies and Procedures: Incident Response Plan

- Define responsibilities of managerial and technical “first responders” in event of breach
- Managerial roles include addressing legal and customer relations issues
- Technical roles include stopping or containing intrusion, restoring data and business operations

Tips on Vendors and Outsourcing

- Know Who They Are
- Know What They Have
- Knew Where They Have It
- Know How They Protect It
- Get Written Commitment

Breach Insurance

- Still a developing area
- Limited history of evaluating risk, so premiums can vary widely
- Scope of coverage can vary widely
- Limits vary and can range from $25,000 to $25 million depending on the nature of the policy and business
- What can be covered?
  - Crisis management services
  - Notification of breached parties
  - Credit/public records/fraud monitoring
  - Fraud remediation services

Data Breach Prevention

Panel Discussion and Q&A

Thank you!

Alan Brill

Senior Managing Director, Kroll Inc.
abrill@kroll.com | 201.770.0400

Alex Gross

Director - Cyber Security and Data Breach Notification, Kroll Inc.
abrill@kroll.com | 201.770.0400

Colin Zick

Partner, *Co-Chair, Privacy & Data Security Practice*
Foley Hoag LLP
czick@foleyhoag.com | 617.832.1275

Michele Whitham

Partner, *Co-Chair, Privacy & Data Security Practice*
Foley Hoag LLP
mwhitham@foleyhoag.com | 617.832.1239

Chris Hart

Associate, Foley Hoag LLP
chart@foleyhoag.com | 617.832.1232

Steve Bychowski

Associate, Foley Hoag LLP
sbychowski@foleyhoag.com | 617.832.1164