Group Legal Services Association

Solo, Small Firm, and General Practice Section

2016 Joint Spring Meeting

May 11-14, 2016, Key West, Florida

Making it Right After a Data Breach and Consumer ID Theft: The Best Way to Keep Your Clients Happy – and Keep Them Yours

---

Friday, May 13
10:30 am – 11:30 am
Salon C-1

Presenter: **Keri Coleman Norris, LegalShield, Ada, OK - Moderator**

Brian Lapidus, Kroll, Nashville, TN

Kroll

USA

Brian Lapidus

Managing Director
Head of Identity Theft and Breach Notification

blapidus@kroll.com

T +1 615.345.9874

100 Centerview Drive
Suite 300
Nashville, TN 37214

EDUCATION & CERTIFICATIONS

- Vanderbilt University, MBA, Strategy and General Management
- Washington University, B.A., Psychology and Business Administration
- Harvard University, Launching New Ventures – Executive Education Certificate

PROFESSIONAL AFFILIATIONS

- Identity Theft Prevention and Identity Management Standards Panel (IDSP)
- International Association of Privacy Professionals (IAPP)

Brian Lapidus is managing director and leader of the Identity Theft & Breach Notification group for the Cyber Security practice of Kroll. Brian has over 15 years of experience leading strategic business development, marketing and product expansion initiatives. His experience includes significant expertise driving affinity marketing programs and enhancing revenue generation for Kroll's membership products.

Brian concurrently focuses on optimizing organizational alignment around these key areas and continues to guide strategic partner relationships into a broader channel marketing structure that has consistently improved business performance. His group is particularly attuned to solutions for healthcare, higher education, retail and financial entities.

Brian's interest in service to higher education may be traced to his early days with the company as the director of strategic products and partnerships for the Background Screening division of Kroll. He created Global Academic Verification (GAV) to assist universities in authenticating foreign student application data matriculating to domestic universities.

In addition to helping business clients resolve issues resulting from data breach, Brian's practice is engaged in consumer-level service and remediation in the wake of such an event. He expanded Kroll's individual identity theft restoration footprint in 2007 when he launched the program in Canada.

Prior to joining Kroll in 2003, Brian developed organizational structures, business processes and performance management programs for offices within the federal government as well as private enterprise.

PROFESSIONAL EXPERIENCE

- **Thought Leadership**
  Recognized as a noted content authority, Brian has contributed by article or interview to various online and print publications, including The Wall Street Journal, Washington Post, New York Times, Chicago Tribune, Bloomberg News, CNN and various media channels. He is also a frequent contributor to the Kroll blog.
- **Speaker and Panelist**
  Brian has been invited to present and moderate at several regional and national conferences, including the IBM IT Services Legal Summit, the International Association of Privacy Professionals (IAPP) Global Privacy Summit, Practical Privacy Series and Privacy Academies, Compliance Week 2011 and LegalTech 2011.

Making it Right After a Data Breach

How to Keep Your Clients Happy, and *Keep Them* As Clients

Brian Lapidus, *Practice Leader*
Identity Theft and Breach Notification

May, 2016

Today's Speaker

About Brian Lapidus

- Practice Leader of the Identity Theft and Breach Notification Group Practice
- Responsible for business development, marketing, operations and product expansion
- Leveraged strategic partner relationships into broader channel marketing structure
- Established vendor management, client services and project management programs for the practice
- Frequent contributor to various media channels, including *The Wall Street Journal*, *Washington Post*, *New York Times*, *Chicago Tribune*, *Bloomberg News* and *CNN*.

Kroll

Today's Discussion

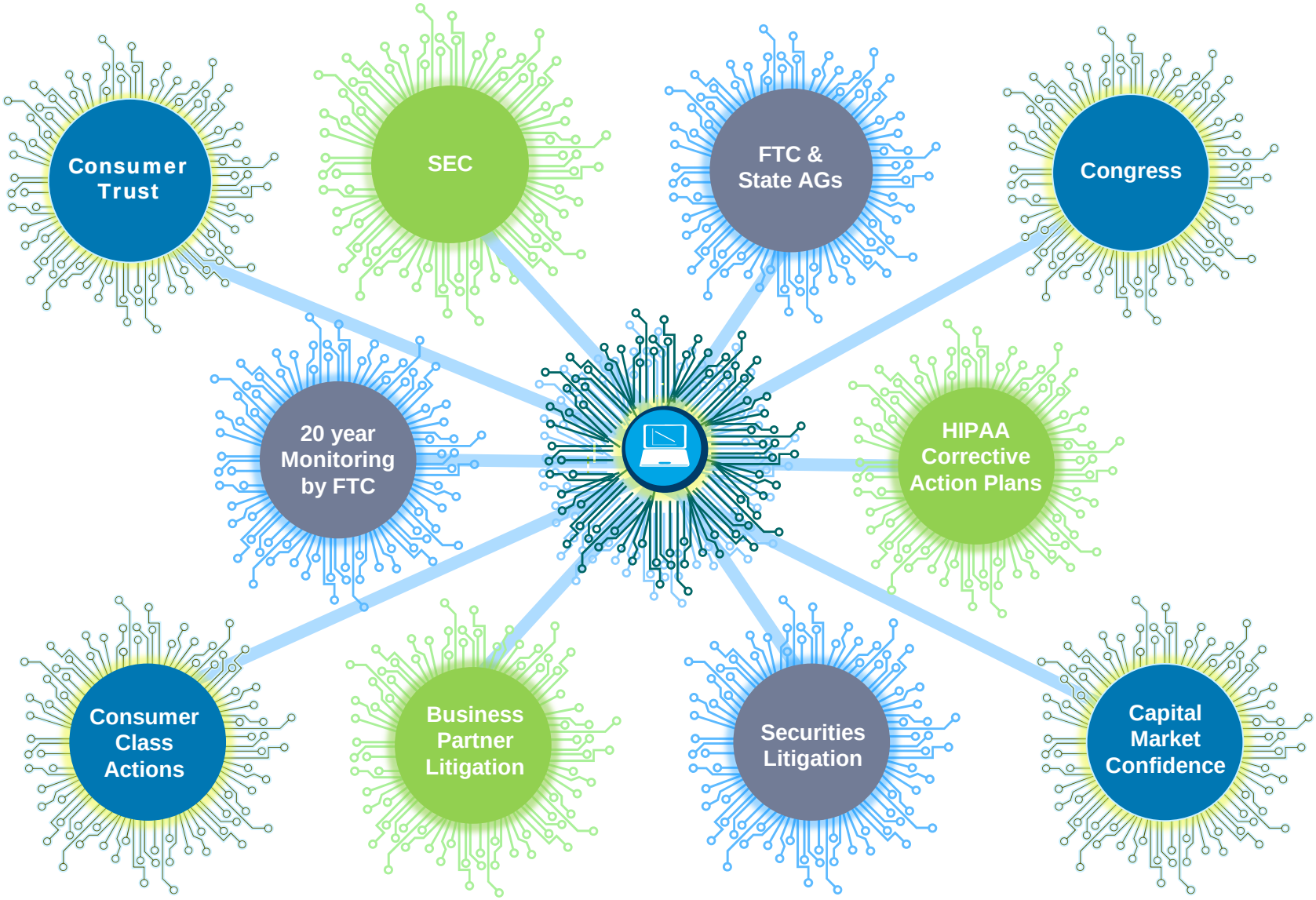
When the personal information of individuals is unexpectedly exposed by an organization, many eyes are watching.

From legislators to shareholders, consumers and shoppers, to patients and students, people expect the wrong to be made right.

- What happens if your client gets it wrong?
- When is expectation ***not*** reality?
- What gives impacted individuals and interested onlookers the most confidence in a company's ability to set things straight and reduce the likelihood of another breach?

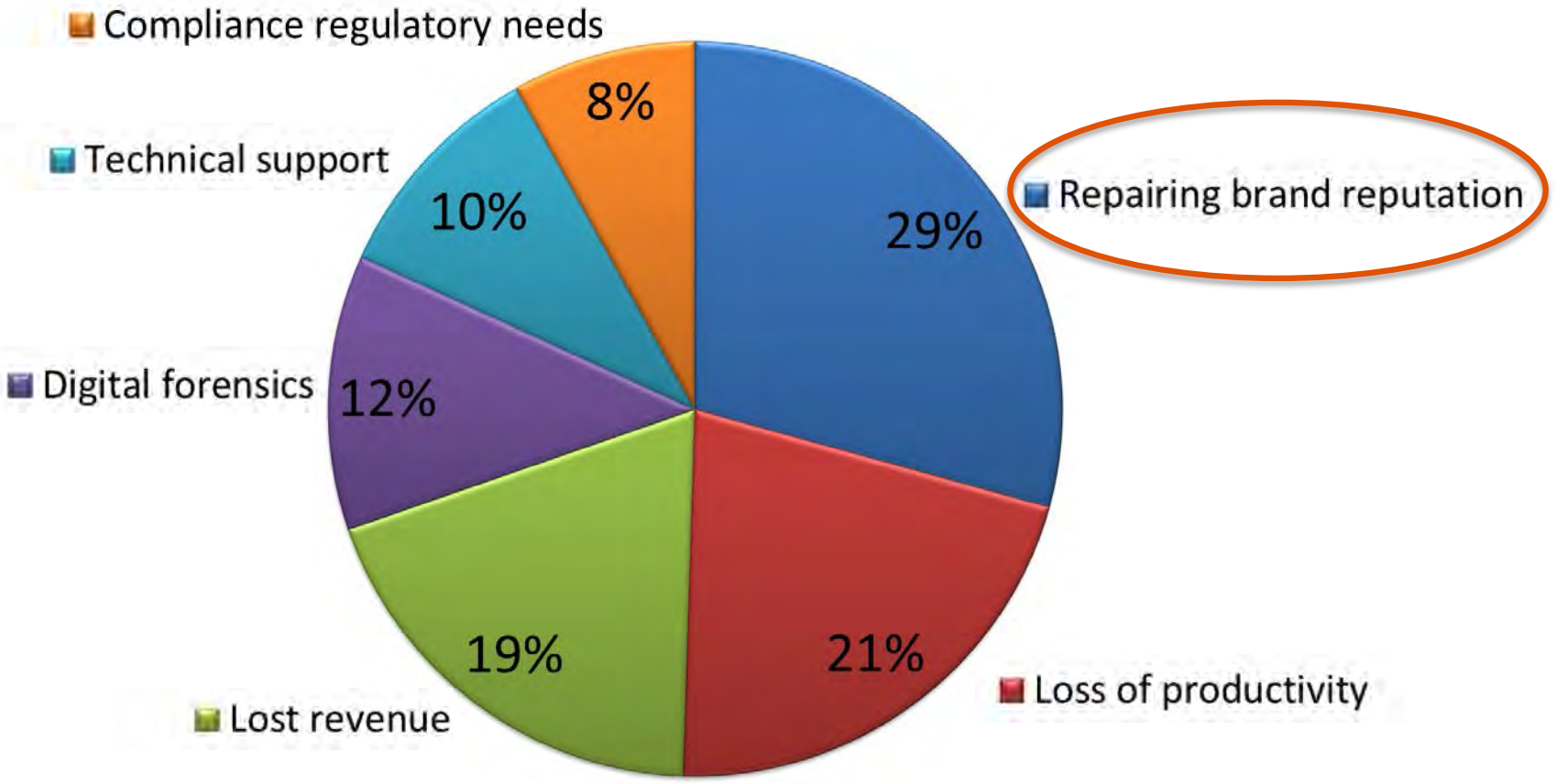
Kroll

Implications of Data Breaches



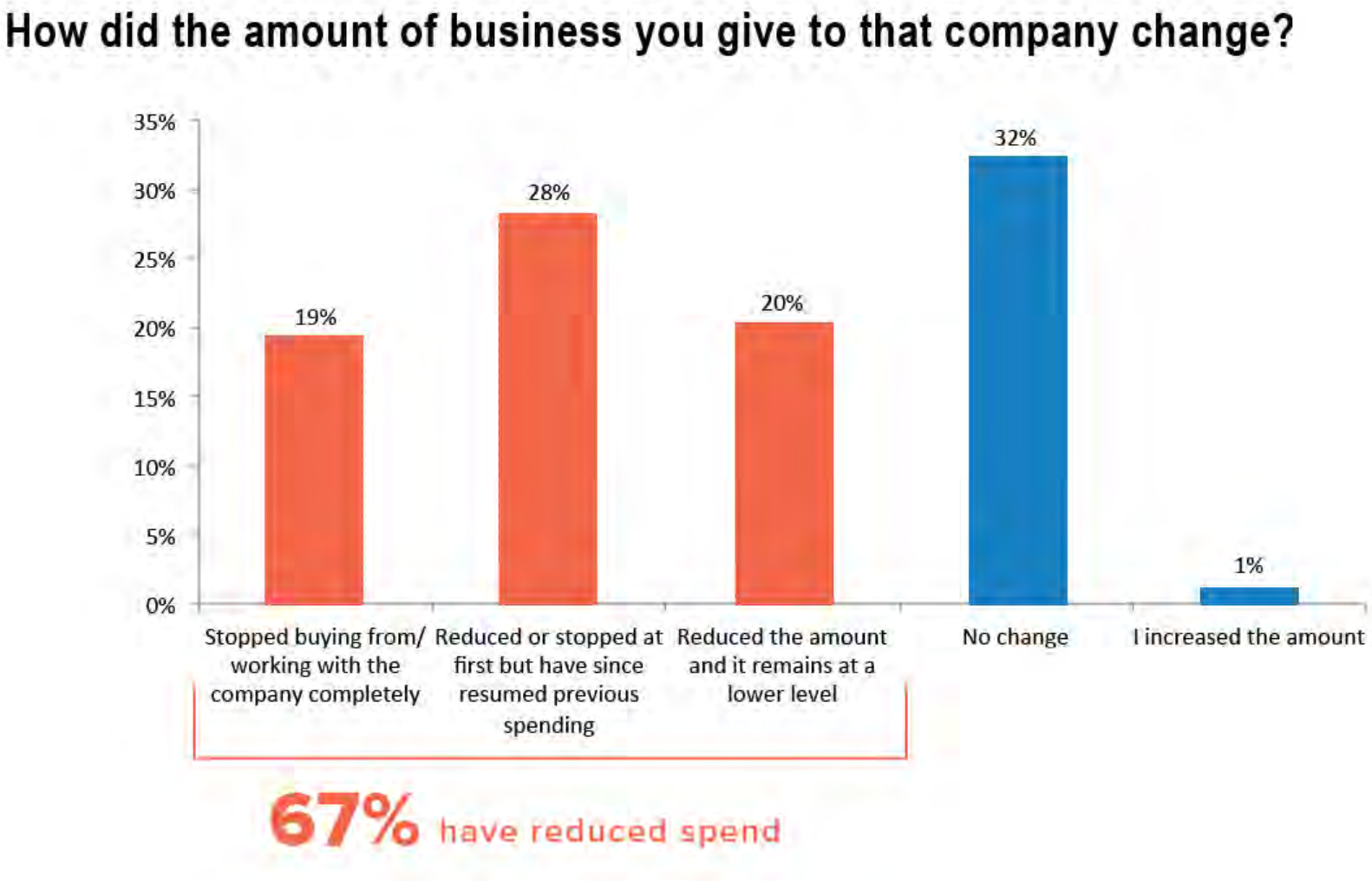
Average data breach cost to a company: $3.5M

And here's where that money goes:



Kroll

Data Breach Changes Victims' Spending Habits

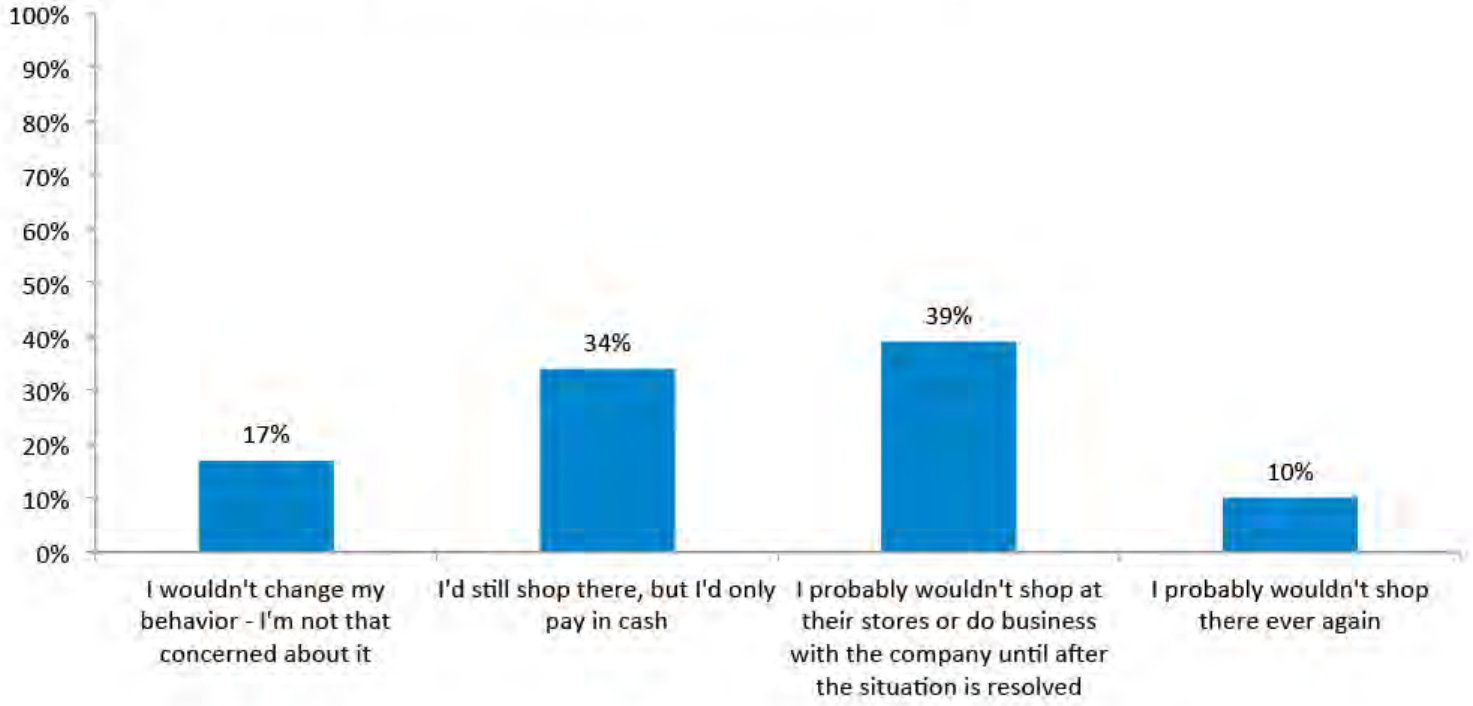


FleishmanHillard TRUE || Issue 11 || Fall, 2015 || Bouncing Back from a Data Hack

Kroll

General consumers stop spending there, too

Which of the following best describes your response upon learning that a company may have been breached, (regardless of whether you've been notified that your own data was compromised)?

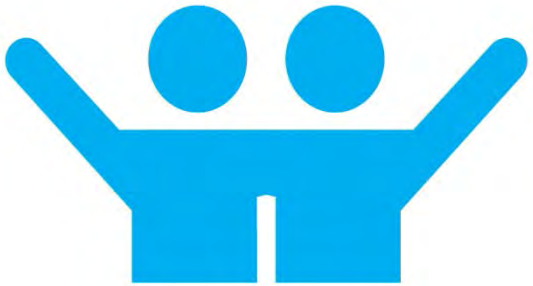


FleishmanHillard TRUE || Issue 11 || Fall, 2015 || Bouncing Back from a Data Hack

Kroll

1 Five Easy Pieces

Kroll



1 **Pick the Right Partners**

2 **Ask the Right Questions**

3 **Offer the Right Remedies**

4 **Illuminate the Steps Taken**

5 **Reconnect with the Audience**

Kroll

Pick the Right Partners

- Recommended and Recognized
- Methodical and Proactive
- Efficient and Quick
- Dedicated and Experienced
- Detailed and Defensible

The Right Direction

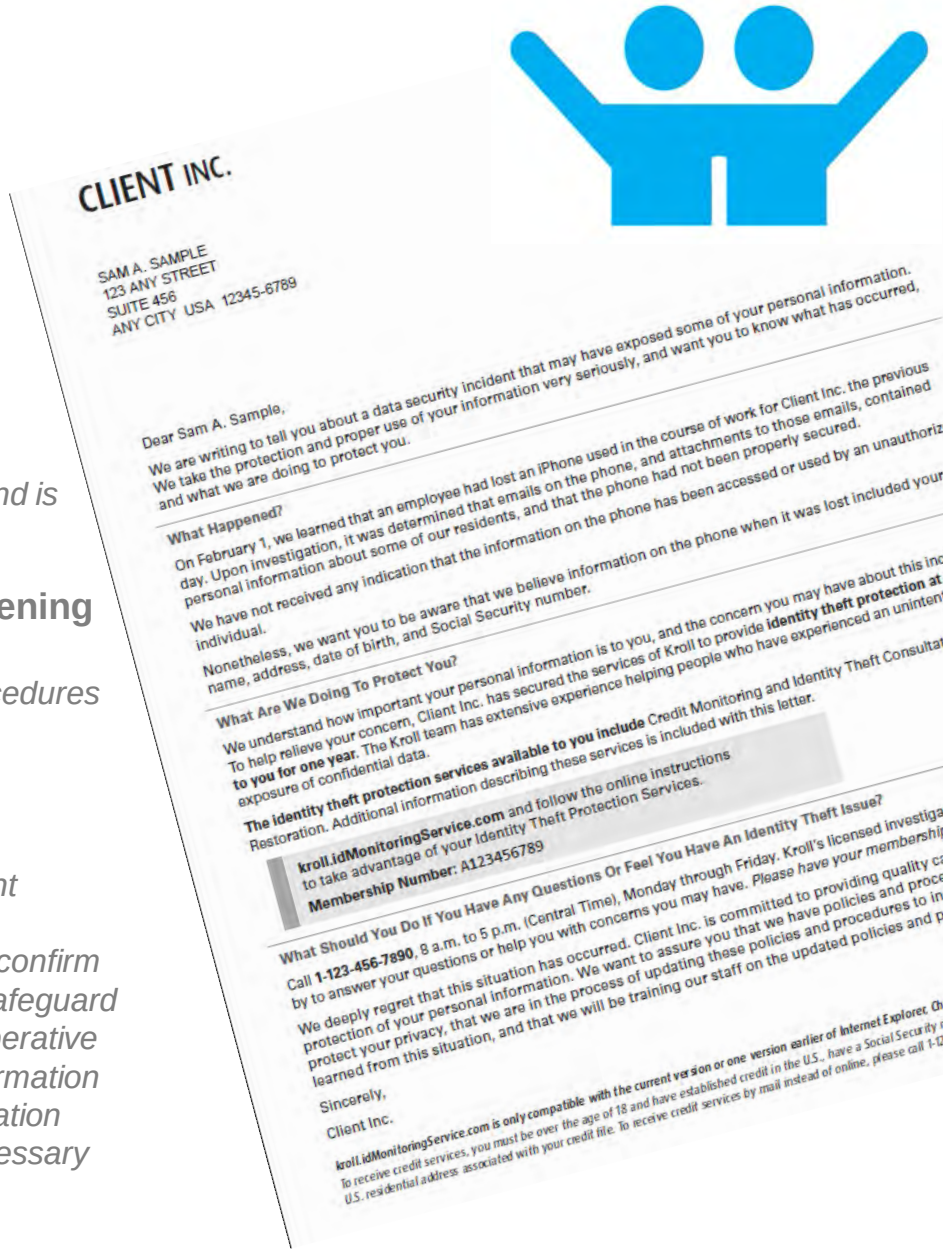
Kroll

When it's Wrong

- Bad breach coaches
- Mixed messages about activating consumer services
- Poor consumer experiences
- Faulty chain of custody
- Sloppy reports
- Round peg, square hole
- Out of control communications

Customized, Compliant Communications

- **When/Where did the theft/breach occur?**
- **What happened? What was lost or stolen?**
- **What is [CLIENT] doing about this?**
  ***SAMPLE**: Client immediately notified local law enforcement and is cooperating with them as they continue their investigation.*
- **What is [CLIENT] doing to prevent this from happening in the future?**
  ***SAMPLE**: [CLIENT] has examined and analyzed existing procedures and systems to ensure appropriate security measures are (reinforced/in place).*
- **Why wasn't I notified sooner?**
  ***SAMPLE**: [CLIENT] immediately notified local law enforcement officials and launched an investigation into the incident. The investigation included a review of internal security systems to confirm that procedures already in place are strengthened to further safeguard against a breach of data security in the future. Last, it was imperative that impacted individuals were identified and their contact information gathered into a consistent format for notification. This investigation was a time-consuming process, but Client believed it was necessary to ensure appropriate precautions and next steps were taken.*



CLIENT INC.

SAM A. SAMPLE
123 ANY STREET
SUITE 456
ANY CITY USA 12345-6789

Dear Sam A. Sample,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously, and want you to know what has occurred, and what we are doing to protect you.

What Happened?

On February 1, we learned that an employee had lost an iPhone used in the course of work for Client Inc. the previous day. Upon investigation, it was determined that emails on the phone, and attachments to those emails, contained personal information about some of our residents, and that the phone had not been properly secured.

We have not received any indication that the information on the phone has been accessed or used by an unauthoriz individual.

Nonetheless, we want you to be aware that we believe information on the phone when it was lost included your name, address, date of birth, and Social Security number.

What Are We Doing To Protect You?

We understand how important your personal information is to you, and the concern you may have about this inc To help relieve your concern, Client Inc. has secured the services of Kroll to provide **identity theft protection at to you for one year**. The Kroll team has extensive experience helping people who have experienced an unintent exposure of confidential data.

The identity theft protection services available to you include Credit Monitoring and Identity Theft Consulta Restoration. Additional information describing these services is included with this letter.

kroll.idMonitoringService.com and follow the online instructions to take advantage of your Identity Theft Protection Services.

Membership Number: A123456789

What Should You Do If You Have Any Questions Or Feel You Have An Identity Theft Issue?

Call **1-123-456-7890**, 8 a.m. to 5 p.m. (Central Time), Monday through Friday. Kroll's licensed investiga by to answer your questions or help you with concerns you may have. Please have your membership

We deeply regret that this situation has occurred. Client Inc. is committed to providing quality c protection of your personal information. We want to assure you that we have policies and proce protect your privacy, that we are in the process of updating these policies and procedures to in learned from this situation, and that we will be training our staff on the updated policies and p

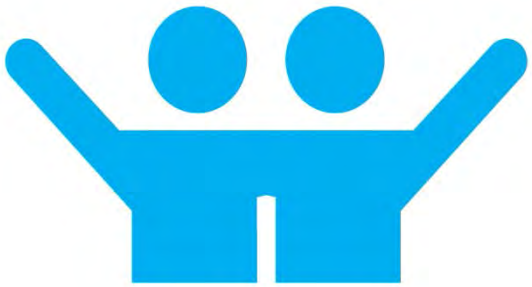
Sincerely,

Client Inc.

kroll.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Ch
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security n U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-1

Kroll

Ask the Right Questions



1 Pick the Right Partners

2 Ask the Right Questions

3 Offer the Right Remedies

4 Illuminate the Steps Taken

5 Reconnect with the Audience

Kroll

Four Factors Get to the Real Risk

1. How did the data breach occur?
2. What was the size of the breach?
3. What type of PII/PHI was exposed?
4. Who is the impacted population?

This stage cannot be underestimated. Only through a prudent analysis of what has happened, how, and to whom, can the nuances of an event be recognized and properly addressed.

Kroll

Consumer Services Decision Factors

1. How did the data breach occur?

- What caused the breach – internal or external actor?
- Was the breach malicious or accidental?
- How did the organization find out about the breach?
- Have any members of the affected population already experienced identity theft?
- What are the regulatory issues that affect the breach?

★ *Here's where Legal Counsel is leveraged, for recommendations and guidance as the breached client weighs these factors. We are not attorneys, and are not giving advice.*

Consumer Services Decision Factors

2. What was the size of the breach?

- What is the total number of records impacted?
- Do you have a stratified population, i.e., is the data exposure different based on varying populations?

Consumer Services Decision Factors

3. What type of PII/PHI was exposed?

- Did you lose data that specifically triggers notification?
- Did you lose data that may not be considered PII under existing law but warrants notification?
- Was this data provided voluntarily by constituents? Was it gathered through providing services or through monitoring the individuals?
- What types of identity theft are tied to the types of data lost?

Consumer Services Decision Factors

4. Who is the impacted population?

- What are the characteristics of the impacted population and their relationship to the organization?
- What is their capacity to protect themselves from financial or personal harm?
- Where do they live?
- What is their relationship to the data?
- Do they include special populations, such as deceased, minors or expatriates?

Kroll

And Speaking of Population …

Be alert to changes

2013

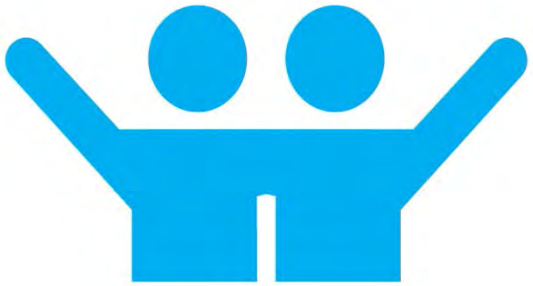
Identity Theft Complaints			
Rank	Victim State	Complaints per 100,000 Population	Complaints
1	Florida	192.9	37,720
2	Georgia	134.1	13,402
3	California	105.4	40,404
4	Michigan	97.1	9,606
4	Nevada	97.1	2,708
6	Maryland	95.5	5,660
7	Arizona	91.2	6,043
8	Texas	88.0	23,266
9	New York	86.9	17,072
10	Illinois	85.9	11,069

2014

Identity Theft Complaints			
Rank	Victim State	Complaints Per 100,000 Population	Complaints
1	Florida	186.3	37,059
2	Washington	154.8	10,930
3	Oregon	124.6	4,946
4	Missouri	118.7	7,195
5	Georgia	112.7	11,384
6	Michigan	104.3	10,338
7	California	100.5	38,982
8	Nevada	100.2	2,846
9	Arizona	96	6,460
10	Maryland	95.9	5,734

https://www.ftc.gov/system/files/documents/ reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf

Kroll



1 **Pick the Right Partners**

2 **Ask the Right Questions**

3 **Offer the Right Remedies**

4 **Illuminate the Steps Taken**

5 **Reconnect with the Audience**

Kroll

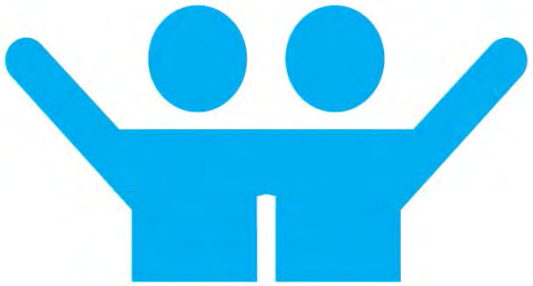
Offer the Right Remedies

Corporate

- Internal Investigation and Interrogatory Interviews
- Data Collection and Preservation
- Data Recovery and Forensic Analysis
- Malware and Advanced Persistent Threat Analysis
- PHI and PII Identification
- Expert Testimony and Reporting

Consumer

- Notice Drafting and Distribution
- Call Center Services
- Credit Monitoring
- Identity Theft Monitoring
- Identity Theft Insurance
- Public Records Monitoring
- Unlimited Consultation and Restoration with a Licensed Investigator



1 **Pick the Right Partners**

2 **Ask the Right Questions**

3 **Offer the Right Remedies**

4 **Illuminate the Steps Taken**

5 **Reconnect with the Audience**

Kroll

Illuminate the Steps Taken

Match remedy to risk.

- Credit monitoring has its place, but can't spot someone's SS# being offered for sale on the black web. Offer meaningful help.

Be thoughtful and clear.

- Crisis communications and Legal counsel can guide notification and media statements, to help ensure a consistent message across all channels.

Transparency Matters

Avoid the blame game.

- To someone whose data was lost by your firm, it doesn't matter if the HVAC supplier or a disgruntled employee was involved. They trusted *you*.

Apologize.

- People don't expect you to be perfect, but they do expect you to be sorry. Empathy goes a long way.

Defensible Proof of Steps, Best Efforts

Kroll

Data Exceptions Report

Total Exceptions Found: 6

CATEGORY		RECORDS FLAGGED	PERCENT OF EXCEPTIONS
Business Names	View	1	16.67%
Duplicates	View	0	0.00%
Incomplete Names	View	0	0.00%
Invalid Address	View	0	0.00%
Possible Duplicates	View	5	83.33%

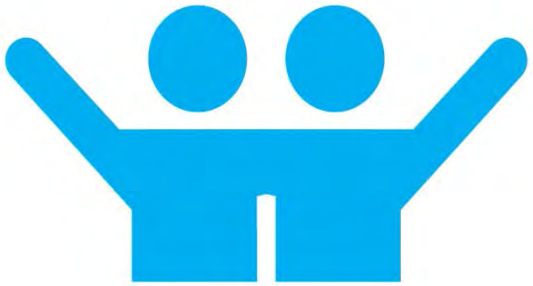
Click the Information Icon for additional details about:

- Accepting Kroll's Recommendations
- Editing Invalid Addresses or Names
- Enrolling Exceptions "As-Is"
- Enabling Macros to View the Report

BUSINESS NAME	
Description	Recommendation

Return to the Summary Page | View All Exceptions (un-sorted)

SID	FIRSTNAME	LASTNAME	ADDRESS1	CITY	STATE	ZIP5	PRIMARYGROUP	EXCEPTION_TYPE
2	MATTHEW	KIDDER	456 BROADWAY	NEWYORK	NY	10009	ADULTS	Possible Duplicate
3	MATT	KIDDER	456 BROADWAY	NEWYORK	NY	10009	ADULTS	Possible Duplicate
4	TIM	OLEARY	123 5TH AVENUE	NEWYORK	NY	10020	ADULTS	Possible Duplicate
5	TIMOTHY	OLEARY	123 FIFTH AVENUE	NEWYORK	NY	10020	ADULTS	Possible Duplicate
6	OLEARY	TIMOTHY	123 FIFTH AVENUE	NEWYORK	NY	10020	ADULTS	Possible Duplicate
7	BRIAN	BANKS	100 CENTERVIEW DR	NASHVILLE	TN	37214	MINOR	Business Name



1 **Pick the Right Partners**

2 **Ask the Right Questions**

3 **Offer the Right Remedies**

4 **Illuminate the Steps Taken**

5 **Reconnect with the Audience**

Kroll

Reconnect

A BULLSEYE VIEW company careers corporate responsibility

updates on Target's security and technology enhancements

April 29, 2014 Since the initial confirmation of the data breach, Target has shared that there has been an active investigation. During that time, we've taken significant actions to further strengthen security across the network. Some of these enhancements include:

Enhancing monitoring and logging
We've implemented additional rules, alerts, centralized log feeds and enabled additional logging capabilities.

Installation of application whitelisting point-of-sale systems
This includes deployment to all registers, point-of-sale servers and development of whitelisting rules.

Implementation of enhanced segmentation
We've developed of point-of-sale management tools, reviewed and streamlined network firewall rules and developed a comprehensive firewall governance process.

Reviewing and limiting vendor access
We've decommissioned vendor access to the server impacted in the breach and disabled select vendor access points including FTP and telnet protocols.

Enhanced security of accounts
We coordinated a reset of 445,000 Target team member and contractor passwords, broadened the use of two-factor authentication, expanded password vaults, disabled multiple vendor accounts, reduced privileges for certain accounts, and developed additional training related to password rotation.

> **I took the one less traveled by,**
> **And that has made all the difference.**

The Road Not Taken
Robert Frost (1874–1963)

Kroll

Contact Details

Brian Lapidus
Practice Leader
Identity Theft and Breach Notification
T + 1 615.577.6770

blapidus@kroll.com