

HOW TO RESPOND TO THE INEVITABLE CYBER- ATTACK



johnreedstark
CONSULTING, LLC



CPE Credits

Today's webcast is worth 1 Continuing Professional Education (CPE) credit.

To be eligible for CPE credit, you must:

- Answer **at least 3 of the 4** polling questions (during the webcast) and have a total viewing time of **at least 50** minutes.
- Participants will have the opportunity to download their CPE certificate immediately following the webcast if above requirements are met.
- In accordance with the standards for the National Registry of CPE Sponsors, CPE credit will be granted based on a 50-minute hour.
- We are unable to grant CPE credit in cases where technical difficulties preclude eligibility. CPE Program Sponsorship guidelines prohibit us from issuing credit to those not verified by the technology to have satisfied the minimum requirements listed above.

HIGH TECH PLUMBER



ROADMAP



INITIAL THOUGHTS



DATA BREACH WORKFLOWS

Death
and
Taxes

Paradigm shift





WHERE TECHNOLOGICAL
INFRASTRUCTURE HAS
EXPANDED DRAMATICALLY

WHERE DATA-POINTS
RESIDE ON MULTIPLE
PLATFORMS



WHERE DATA
BREACHES DON'T
DEFINE VICTIM
COMPANIES; HOW
THEY RESPOND TO
THEM DOES

IR SEQUENCE OF EVENTS

RECON

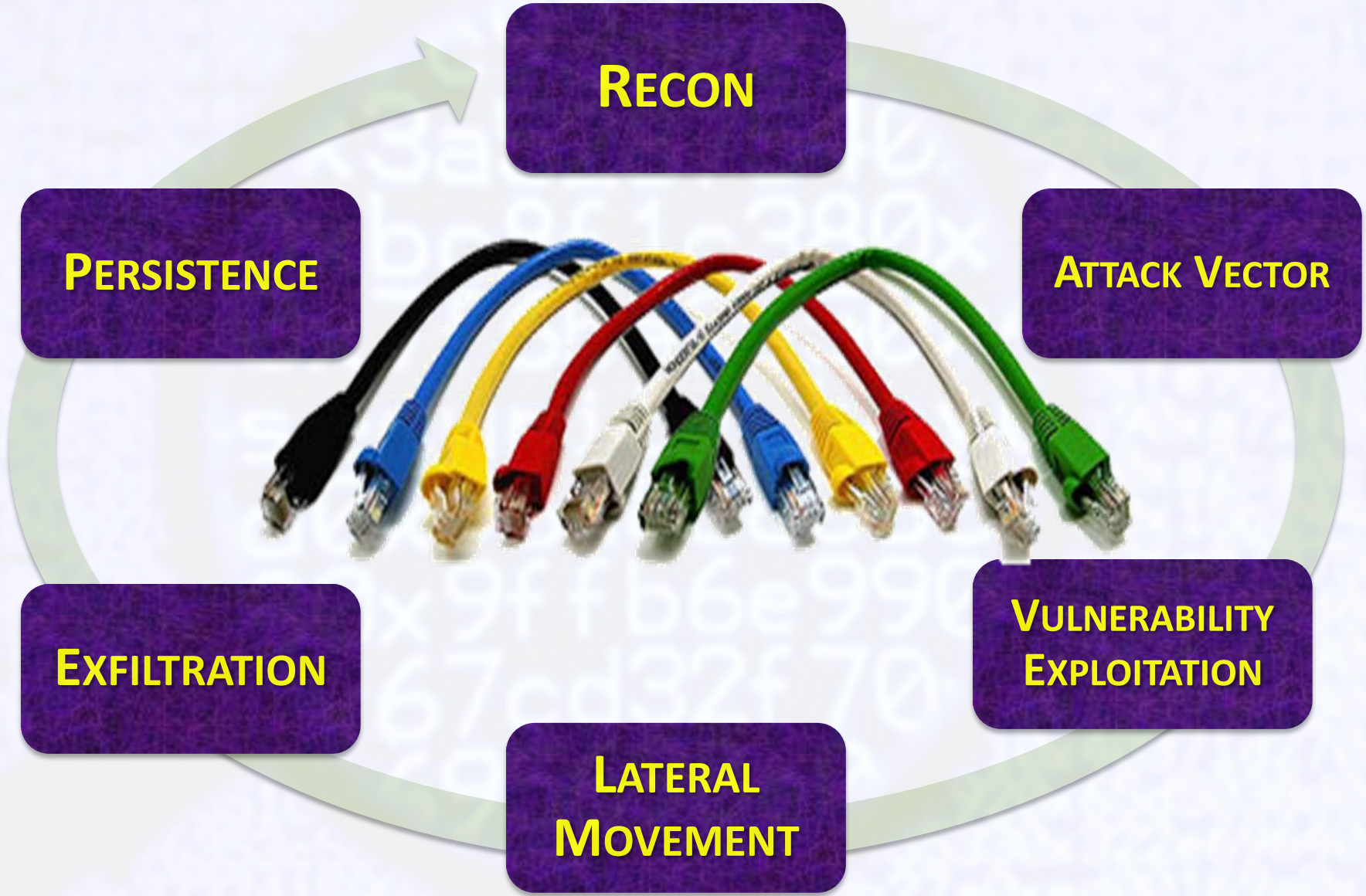
ATTACK VECTOR

**VULNERABILITY
EXPLOITATION**

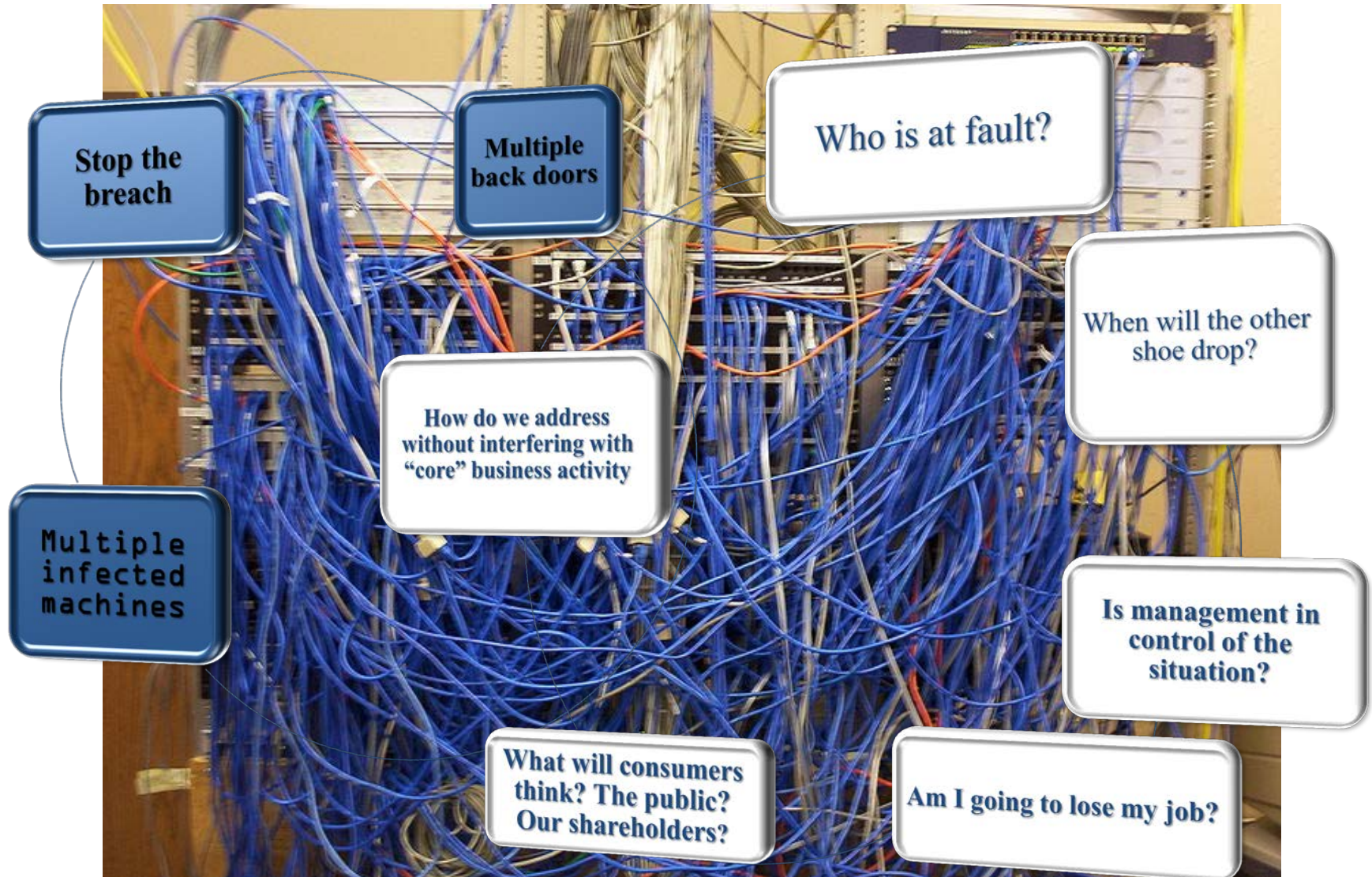
**LATERAL
MOVEMENT**

EXFILTRATION

PERSISTENCE



TYPICAL DAY ONE STATE-OF-PLAY





#1



**HOT
TIP**

PRESERVE, ETC.

ASSEMBLE TEAM, DISTRIBUTE LIST OF RESPONSIBILITIES

UNHOOK INFECTED MACHINES

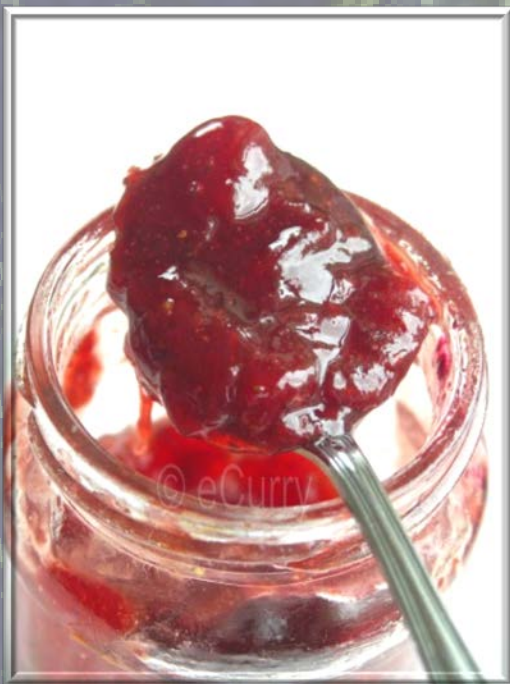
CALL OUTSIDE EXPERTS TO FORENSICALLY IMAGE

PULL NEEDED BACKUPS OUT OF ROTATION AND INSERT CLEAN AND PATCHED MACHINES

SAVE OFF LOG FILES, KEYCARD DATA AND SURVEILLANCE TAPES

START REAL-TIME NETWORK PACKET CAPTURE

FORCE ADMINISTRATOR AND USER PASSWORD CHANGE

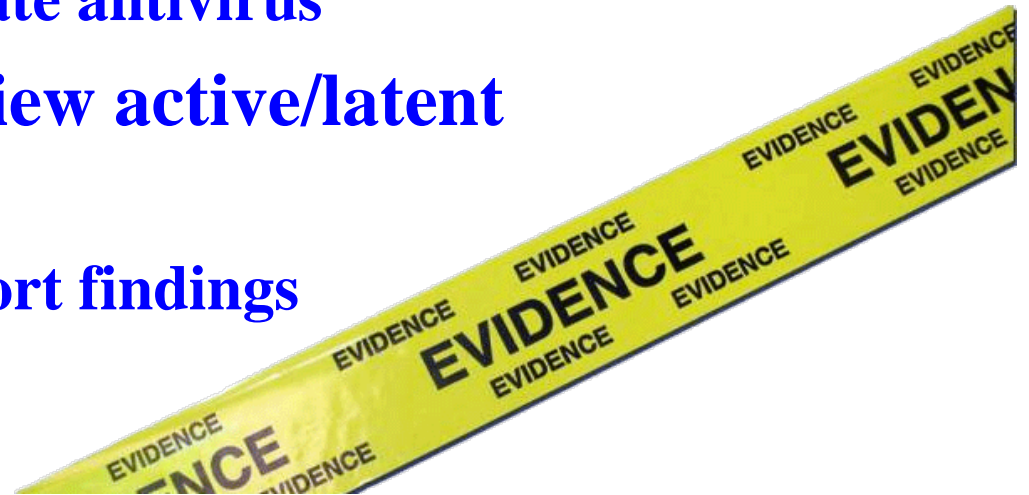




PRESERVATION CHALLENGES

COORDINATING IT AND PRESERVATION ACTIVITY

- **IT needs to secure data environment**
 - Pull network connection, save backups and logs, prepare clean “builds,” force password change, update antivirus
- **Forensics needs to review active/latent data**
 - Image servers and report findings



2

DIGITAL FORENSIC ANALYSIS

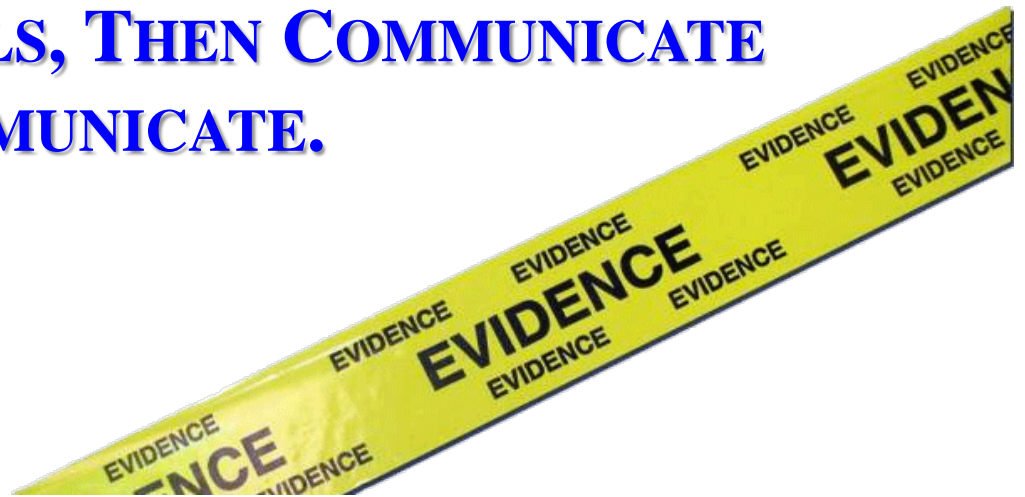




COORDINATION CHALLENGES

COORDINATING IT AND FORENSIC ACTIVITY

- **IT NEEDS TO SECURE DATA ENVIRONMENT**
- **FORENSICS NEEDS TO REVIEW AND ANALYZE DATA**
- **BUT CORE BUSINESS ACTIVITY MUST CONTINUE**
- **ESTABLISH PROTOCOLS, THEN COMMUNICATE
COMMUNICATE, COMMUNICATE.**



3

LOGGING ANALYSIS





4

MALWARE REVERSE ENGINEERING





5

SURVEILLANCE





6

REMEDIATION EFFORTS



data breach protections do not detect quickly enough, or act nimbly enough, to counter today's sophisticated and clandestine data breaches.



John Reed Stark

Yet, so many companies remain unwilling to recalibrate cyber-security into a more effective arche-

are important cyber-security measures. But everyone knows that already. Let's focus on what everyone does not already know.

Ever Heard of EDRs?

Recently, a wave of dedicated incident response solutions known as "end-point detection and response" or "EDR" tools have come into being. Typically installed within a swath of IT equipment including domain controllers, database

down, and a range of other risk-related analytics. Purchasing cyber-insurance is much different, however, because no standard policies exist and the cyber-insurance market remains in its infancy, leading many companies to forego available policies and rely upon their more traditional policies of general liability and property. This is backwards thinking.

Instead, management should undertake an approach towards its insurance calculus based more upon data breach re-

Conventional cyber-security fortification and defense measures need to make way for EDRs; otherwise companies risk a sluggish, incomplete and piecemeal data breach investigation.

that somebody screwed up and left a door unlocked. This only further fuels the fire that breached companies must redouble fortification and detection. That might be true, but the reality is that companies, above all else, should pivot their attention and focus to data breach response."

In other words, when companies trying to prevent data breaches rely too much

activity on enapoints and servers, EDR

a company can then collaborate with its

Conventional cyber-security fortification and defense measures need to make way for EDRs; otherwise companies risk a sluggish, incomplete and piecemeal data breach investigation.



7

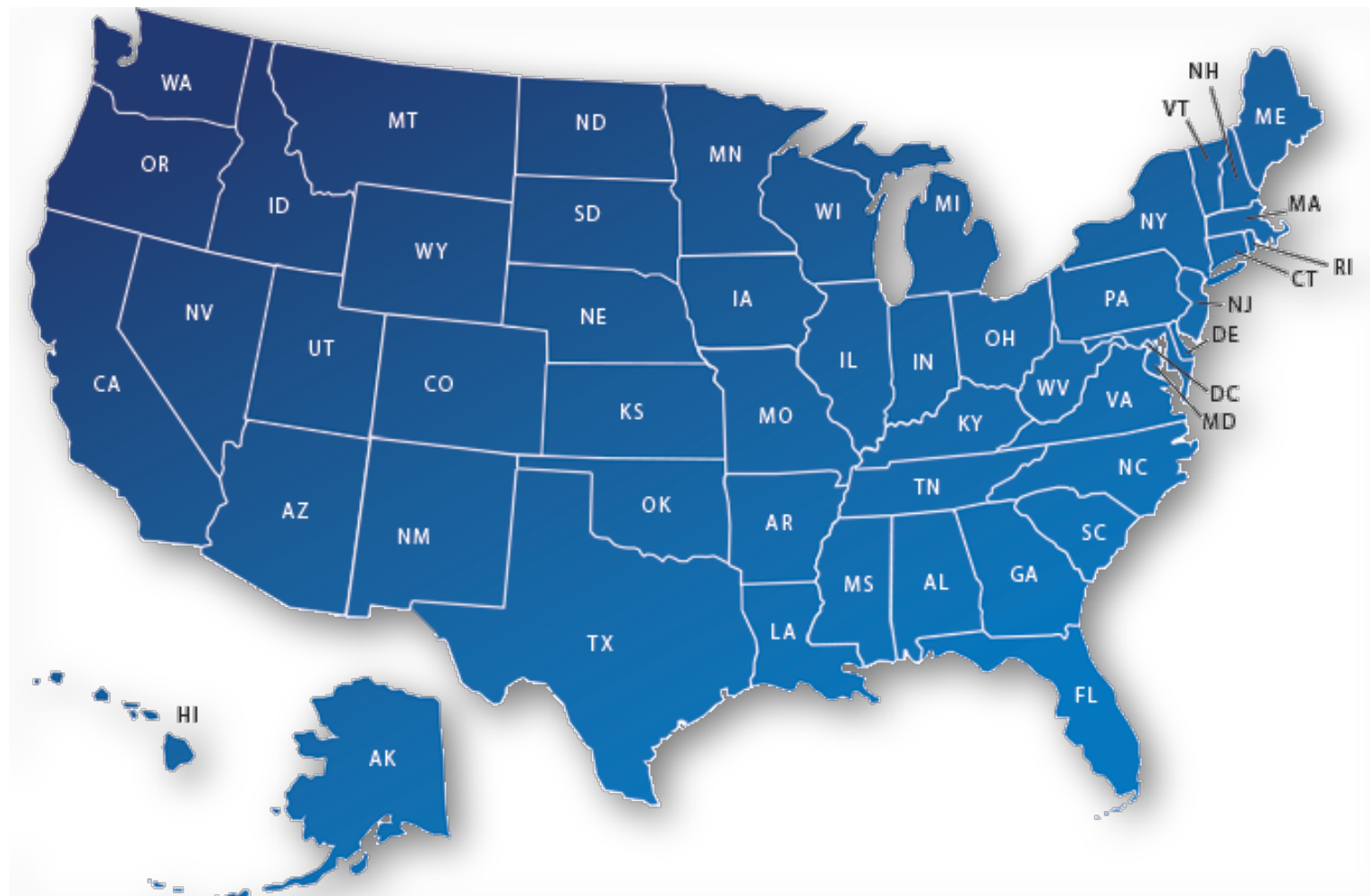
EXFILTRATION ANALYSIS





8

STATE REGULATORY COMPLIANCE





9

FEDERAL REGULATORY COMPLIANCE





PCI COMPLIANCE

PCI Compliance



Interfacing with Brands



PVEDMALL.COM

- Contractually bound to hire an investigator “PFI”
- Careful!!! The investigator will be beholden to the brand or regulatory agency – not your company!

Remember the Big Picture



PVEDORALL.COM

- Often First Outsider To Look At Company's Response
- PFI Report Likely Not Privileged
- Positions Taken Might Impact Other Workflows



11

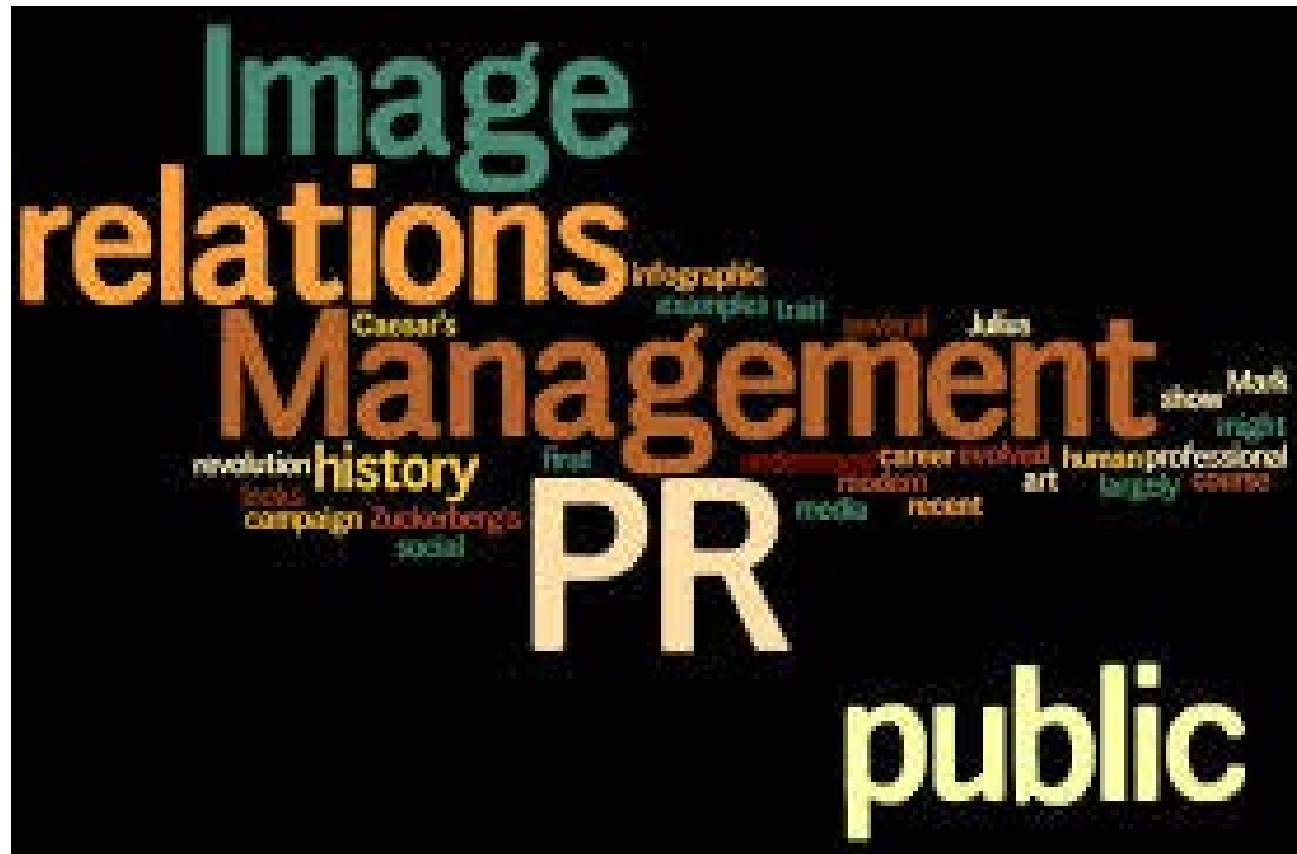
LAW ENFORCEMENT LIAISON





12

PUBLIC/CONGRESSIONAL RELATIONS



13

CONSTITUENCY NOTIFICATIONS

We ♥ Our Customers



EMPLOYEE ENGAGEMENT



VENDORS WANTED



CONSTITUENCY NOTIFICATION: PARTNERS



CONSTITUENCY NOTIFICATION: INSURANCE CARRIER



CONSTITUENCY NOTIFICATION: BOARD OF DIRECTORS



CONSTITUENCY NOTIFICATION: 3RD PARTY VENDORS



CONSTITUENCY NOTIFICATION: GOVERNMENT

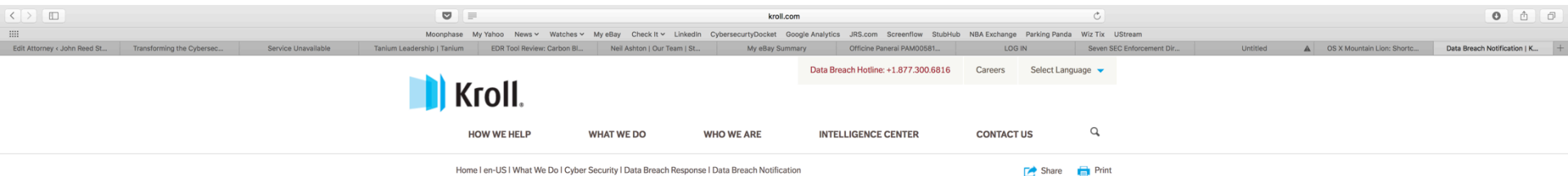


National Association
of Attorneys General

CONSTITUENCY NOTIFICATION: EMPLOYEES



CONSTITUENCY NOTIFICATION: CUSTOMERS



Data Breach Notification

Kroll's data breach notification solutions — from drafting compliant letters, to full-service mailing help, to alternate notifications for large breaches — take the burden off your organization.

With Kroll's data breach notification team, you'll have the support you need to get the right information to the right people at the right time. We will work closely with you to optimize speed and deliverability while also reducing unnecessary notification costs.

Our breach notification specialists have assisted clients across diverse industries with their notification responsibilities. As such, we understand how different industries—especially highly regulated ones—have distinct obligations and varied levels of risk. We'll help you and your counsel draft data breach notices so that your messages are timely, cost-effective, and appropriate to the [sensitivity of the data](#) and audience involved.

Kroll offers templates and direct assistance to make the process of drafting a [notification letter](#) easier for the organization and their legal counsel. This can be used as a starting point for customization to ensure the letter meets all standard requirements while still addressing the needs of each affected party.

You and your legal counsel can rely on Kroll's reputation for delivering positive messaging tailored to the impacted audience that explains the data breach event while preserving brand integrity. We'll leave the individuals impacted by your breach feeling confident and protected — knowing that if identity theft or fraud does occur, our licensed identity theft investigators will be there to help them handle the situation quickly and effectively.

If sending notification letters isn't appropriate or possible, Kroll offers alternative notification methods. Working with your legal counsel, PR/communications, or other members of your response team, Kroll can facilitate distribution of email notifications or public notifications in instances where contact information is not known, or the population is too large for print notification. Kroll can build a website to help facilitate the notice to the public and to assist in monitoring services enrollment.

In an increasingly treacherous cyber security landscape, it's always best to be prepared for a data breach. With Kroll, you can be confident that experts are standing by to partner with your company's leadership and your legal counsel — putting you in the best defensible position in the event of a data breach.

Cyber Security Capabilities

Cyber Crime Investigations	>
Data Breach Prevention	>
Incident Response Management	>
Data Breach Response	>
Cyber Litigation Support	
Cyber Due Diligence	
IDShield Powered By Kroll	

Suspect a Data Breach?

We offer immediate, 24/7 assistance from our team of data breach experts via our Data Breach Hotline.

Call the Data Breach Hotline
1.877.300.6816

[CONTACT US ONLINE](#)

Experts Spotlight



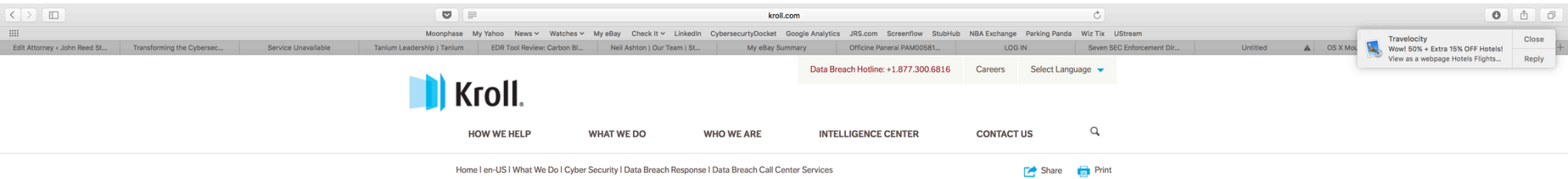
Brian Lapidus
MANAGING DIRECTOR,
IDENTITY THEFT AND BREACH
NOTIFICATION

[+1 615.577.6770](#) | [Email](#)

[SEE ALL](#)

[CONTACT US](#)

CONSTITUENCY NOTIFICATION: CALL CENTER



Data Breach Call Center Services

A [notification letter](#) can generate lots of questions for those affected by a data breach. Krill's call center services are provided by skilled representatives who know how to handle difficult questions and stand at the ready to serve your breached population.

Sometimes a real conversation can go a long way in easing concerns about a data breach event. That's why our multilingual customer support team is ready quickly to provide front-line care for affected individuals. There's no scrambling to assemble and train a team — our skilled, background-checked staff is already in place, prepared to serve your breached audience right away.

Our call center team is capable of answering thousands of inquiries quickly and professionally to help you maintain stakeholder trust. We'll work with you to create a data breach notification FAQ customized to your business and industry, allowing our support team — devoted to handling calls about your incident — to function as a seamless extension of your company. Our data breach notification call center also provides access to Krill's [licensed investigators](#), who can help individuals affected by a breach with questions about identity theft, and assist with personalized safeguards to reduce the likelihood of financial impact from unauthorized use of their lost or exposed data.

Should a breach include special populations, such as minors, decedents, or expatriates, consultation from an experienced support team will be important in resolving the questions from family members responsible for their loved ones.

In data breach response, the role of the call center is to ease fears, reduce confusion, and answer questions about the benefits available and the solutions in place. You'll rest assured knowing that Krill's team, having supported countless breaches with thousands of hours of experience, is well equipped to provide the right level of service on behalf of your organization.

Cyber Security Capabilities

Cyber Crime Investigations	>
Data Breach Prevention	>
Incident Response Management	>
Data Breach Response	>
Cyber Litigation Support	
Cyber Due Diligence	
IDShield Powered By Krill	

Suspect a Data Breach?

We offer immediate, 24/7 assistance from our team of data breach experts via our Data Breach Hotline.

Call the Data Breach Hotline
1.877.300.6816

[CONTACT US ONLINE](#)

Experts Spotlight



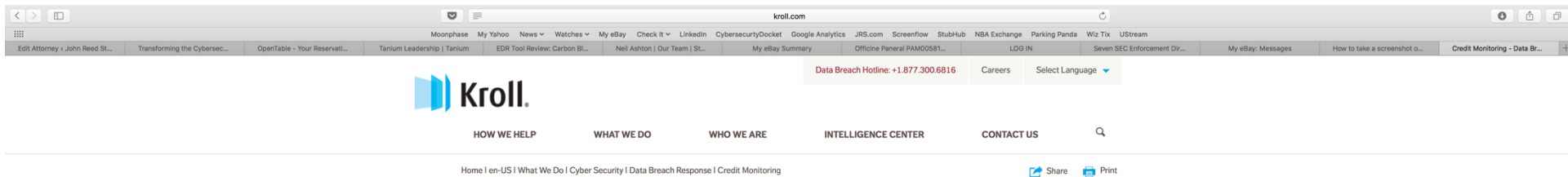
Brian Lapidus
MANAGING DIRECTOR,
IDENTITY THEFT AND BREACH
NOTIFICATION

[+1 615.577.6770](#) | [Email](#)

[SEE ALL](#)

[CONTACT US](#)

CONSTITUENCY NOTIFICATION: CREDIT MONITORING



Credit Monitoring

Credit monitoring can be a powerful tool to offer in the [wake of a data breach](#). Kroll provides a monitoring alert system that's backed by the expertise of our licensed investigator team.

As the world's leading provider of end-to-end cyber security services, Kroll offers a unique, holistic solution for data loss events, including facilitating access to credit reports and credit monitoring. For your company's breached audience, identity credit monitoring can provide a meaningful tool to assist individuals in detecting the signs of identity theft that include fraudulent credit activity. When a breach occurs, we'll work with you to determine exactly what data was breached, and if credit monitoring is the right solution for your customers.

Quite simply, monitoring credit is a tool that alerts consumers when changes have occurred to their credit profile. Kroll's continuous credit monitoring service will notify the customer if certain activity is reported, including inquiries, new trade-lines, derogatory notices, public records, and changes of address – those most commonly associated with suspicious activity that may indicate the presence of identity theft. When changes occur, consumers can easily see whether the change is legitimate or whether it represents potential fraudulent activity. This monitoring can occur with one bureau only, or across all three.

Kroll's [licensed investigators](#) can help walk individuals through the process of reading their credit report, analyzing their credit data, and spotting evidence of identity theft or fraud. Individuals who believe unauthorized actions have been taken can also consult our licensed investigators to help determine if they are [experiencing an identity theft](#) issue.

Cyber Security Capabilities

Cyber Crime Investigations	>
Data Breach Prevention	>
Incident Response Management	>
Data Breach Response	>
Cyber Litigation Support	
Cyber Due Diligence	
IDShield Powered By Kroll	

Suspect a Data Breach?

We offer immediate, 24/7 assistance from our team of data breach experts via our Data Breach Hotline.

Call the Data Breach Hotline
1.877.300.6816

[CONTACT US ONLINE](#)

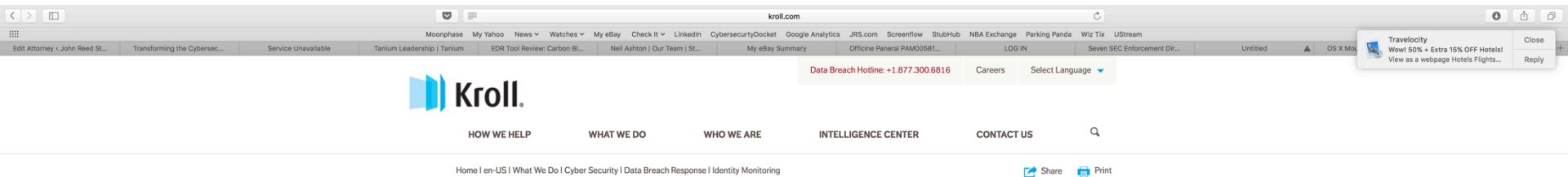
Experts Spotlight



Brian Lapidus
MANAGING DIRECTOR,
IDENTITY THEFT AND BREACH
NOTIFICATION
[+1 615.577.6770](#) | [Email](#)

[SEE ALL](#)

CONSTITUENCY NOTIFICATION: IDENTITY MONITORING



Identity Monitoring

Kroll's unique combination of identity monitoring services can detect more types of identity theft than credit monitoring alone, providing practical help to combat identity theft and fraud.

Did you know that very few cases of identity theft—as few as two in 10—can be detected on a credit report?

Because [credit monitoring](#) is not a useful tool when certain types of data are compromised, an organization may choose to offer identity monitoring to provide consumers with insight into many different aspects of a consumer's identity that can reveal known triggers of identity theft that credit monitoring alone would not.

Identity monitoring provides data associated with an individual's non-credit-based [personally identifiable information \(PII\)](#), and reports information that is not tracked by credit bureaus. This type of monitoring can look for information in public records, or it may be searching for instances of PII found on the Internet, particularly sites known for illegal sales of PII.

Kroll's identity monitoring services provide web-based monitoring of PII including:

- Social Security Number/National ID Number
- Bank Account Number
- Bank Routing Number
- Credit/Debit Cards
- Medical ID Numbers
- Email Address
- Phone Number

Identity Monitoring: Offering individuals peace of mind

Kroll's identity monitoring services instantly notify affected individuals by email of any activity related to their personal information. Individuals then have the opportunity to review the information and take appropriate steps if the information is deemed inaccurate or if it is indicating identity theft or fraud.

Cyber Security Capabilities

Cyber Crime Investigations	>
Data Breach Prevention	>
Incident Response Management	>
Data Breach Response	>
Cyber Litigation Support	
Cyber Due Diligence	
IDShield Powered By Kroll	

Suspect a Data Breach?

We offer immediate, 24/7 assistance from our team of data breach experts via our Data Breach Hotline.

Call the Data Breach Hotline
1.877.300.6816

[CONTACT US ONLINE](#)

[Error loading the WebPart 'IDShieldCallout' of type 'IDShieldCallout']

Experts Spotlight



Brian Lapidus
MANAGING DIRECTOR,
IDENTITY THEFT AND BREACH
NOTIFICATION
[+1 615.577.6770 | Email](#)

[SEE ALL](#)

[CONTACT US](#)

CONSTITUENCY NOTIFICATION: ID THEFT RESTORATION

The screenshot shows the top portion of the Kroll website. At the top, there is a navigation bar with the Kroll logo on the left and a search icon on the right. Below the logo, the text "HOW WE HELP", "WHAT WE DO", "WHO WE ARE", "INTELLIGENCE CENTER", and "CONTACT US" is displayed. A search icon is also present. Below the navigation bar, there is a secondary navigation bar with the text "Home | en-US | What We Do | Cyber Security | Data Breach Response | Identity Theft Restoration". On the right side of this bar, there are icons for "Share" and "Print".

Identity Theft Restoration

Kroll provides your breach population with direct access to investigative experts for live support and best practice advice, as well as identity restoration should they become victims of identity theft.

[Identity monitoring services](#) are great tools for individuals impacted by a breach, but they can't deliver the same kind of reassurance and customized advice one gains from speaking with an expert. The last thing you want is to leave your affected employees, members, students or customers alone to deal with the potential consequences of a breach of data that you were responsible for protecting – especially in the event that those consequences lead to identity theft.

Live support when consumers have questions

How reassuring would it be to know that you could pick up the phone and speak directly with your doctor at the first twinge of pain or sign of a cold? That's the kind of reassurance Kroll provides your breach population, as they can pick up the phone and speak with a knowledgeable licensed investigator who can directly address their specific situation – someone whom they can establish a relationship with should they ever experience identity theft. We investigate the suspicious activity and offer recommendations and best practice advice while directly assisting the individual.

In-depth identity theft restoration when consumers become victims

Identity theft can be a nightmare that the average consumer is ill-equipped to deal with. Luckily, Kroll's licensed identity theft investigators are available as your partners for identity theft restoration – restoring compromised identities to pre-breach status, and preserving faith in your business.

In order to best assist individuals impacted by a breach, Kroll's licensed investigators receive intensive training that enables them to provide individuals with the tools they need to combat any form of identity theft or fraud. Our investigators have ability to do the majority of the work required to restore an identity on an individual's behalf, helping them gain the peace of mind that comes with knowing the most experienced identity theft restoration professionals are on

Cyber Security Capabilities

Cyber Crime Investigations	>
Data Breach Prevention	>
Incident Response Management	>
Data Breach Response	>
Cyber Litigation Support	
Cyber Due Diligence	
IDShield Powered By Kroll	

Suspect a Data Breach?

We offer immediate, 24/7 assistance from our team of data breach experts via our Data Breach Hotline.

Call the Data Breach Hotline
1.877.300.6816

[CONTACT US ONLINE](#)

[Error loading the WebPart 'IDShieldCallout' of type 'IDShieldCallout']

Experts Spotlight



Brian Lapidus
MANAGING DIRECTOR,
IDENTITY THEFT AND BREACH
NOTIFICATION

+1 615.577.6770 | [Email](#)

[SEE ALL](#)

[CONTACT US](#)



