

Data Breach Response: Working With Attorneys and Regulators

Stephen Reynolds, CISSP, CIPP/US
Partner at Ice Miller LLP

Douglas Swetnam, CIPP/US
*Section Chief Data Privacy & Identity Theft Unit,
Office of the Indiana Attorney General*



Today's Topics

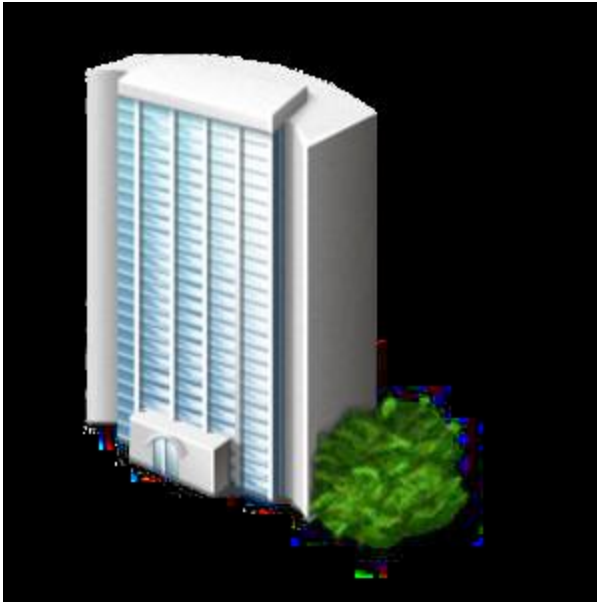
1. Cyber-Crime: An Overview
2. Breach Response . . .
 - A. What do the lawyers do?
 - B. What do the regulators do?
 - C. How can we all work together?

CYBER-CRIME: TOP THREATS

- Fund Transfer Fraud
- Ransomware
- Malicious Insiders
- W-2 Phishing Scams
- Data Breaches



FUND TRANSFER FRAUD – WHAT IS IT?



WHAT IS AT RISK?



Losses reported to law enforcement from October 2013 to August 2015 were over **\$1.2 billion**.

WHAT DOES IT LOOK LIKE?

From: CEO, Joe <joe.ceo@yourcompany.com>
Sent: Sunday, September 13, 2015 2:58 PM
To: CFO, Jim
Subject: Important Request
Importance: High

Hello Jim,

Can you please email me the details you will need to help me process an outgoing wire transfer to another bank. Please kindly note that I can't take calls right now due to meetings, therefore, I will appreciate swift email correspondence.

Hope I am not bothering you too much with this?

Thanks,

Joe

FUND TRANSFER FRAUD LIABILITY

Uniform Commercial Code Article 4A

- Liability falls to customer if the bank has adopted a commercially reasonable security procedure, and the bank has followed that procedure in good faith.

What constitutes “commercially reasonable?”

- Some courts have looked to industry standards and industry white papers (e.g. *Federal Financial Institutions Examination Council – Authentication in an Internet Banking Environment*)

RANSOMWARE



MALICIOUS INSIDERS



MALICIOUS INSIDERS

Employee of Law Firm Wilson Sonsini Charged With Insider Trading

By MATTHEW GOLDSTEIN SEPTEMBER 16, 2014 2:48 PM 5

Email

Share

Tweet

Save

More



In 2011, federal prosecutors charged Matthew Braverman with taking part in an insider trading conspiracy.

Federal authorities, for the second time, charged an employee of Wilson Sonsini Goodrich & Patton, a law firm, with using confidential information to make illegal trades in stocks.

Dmitry Braverman, an information technology engineer at Wilson Sonsini, was charged Tuesday with using confidential information to make illegal trades in stocks. Braverman, 41, was arrested by F.B.I. law enforcement spokesman said.

LAW360

News, cases, companies, firms



Advanced Search

Ex-Locke Lord IT Engineer Gets 9.5 Years For Network Attack

By Jess Davis

Share us on: [Twitter](#) [Facebook](#) [LinkedIn](#) [Email](#)

Law360, Dallas (April 15, 2016, 4:54 PM ET) -- A former Locke Lord LLP information technology engineer convicted of felony computer intrusion for attacks on the firm's network in 2011 was sentenced Thursday to about 9.5 years in jail and ordered to pay \$1.7 million in restitution, according to the U.S. Department of Justice.

Anastasio N. Laoutaris, 41, is a former engineer for the firm, who was charged with two felony counts stemming from his alleged December 2011 attacks on the firm's computer system. A Texas federal jury in September found Laoutaris guilty, and U.S. District Judge Jane Boyle sentenced him Thursday to 115 months in prison and ordered him to pay \$1.697 million in restitution, according to U.S. Attorney John Parker.

According to court records, Laoutaris was a senior systems engineer for Locke Lord from March 2006 to August 2011. In December 2011, he allegedly twice accessed the firm's computer network and on both occasions, took steps that "caused significant damage to the network," including deleting or disabling hundreds of user accounts, desktop and laptop accounts and user e-mail accounts.

Locke Lord spokeswoman Julie Gilbert said Friday the firm was "attacked — not hacked." No firm or client information was lost or disclosed to unauthorized parties, and though some of the firm's systems were down, none of its data were compromised, she said.

[Add to Briefcase](#)
[Printable Version](#)
[Rights/Reprints](#)
[Editorial Contacts](#)

Related

Sections
[Legal Industry](#)

Law Firms

[Locke Lord](#)

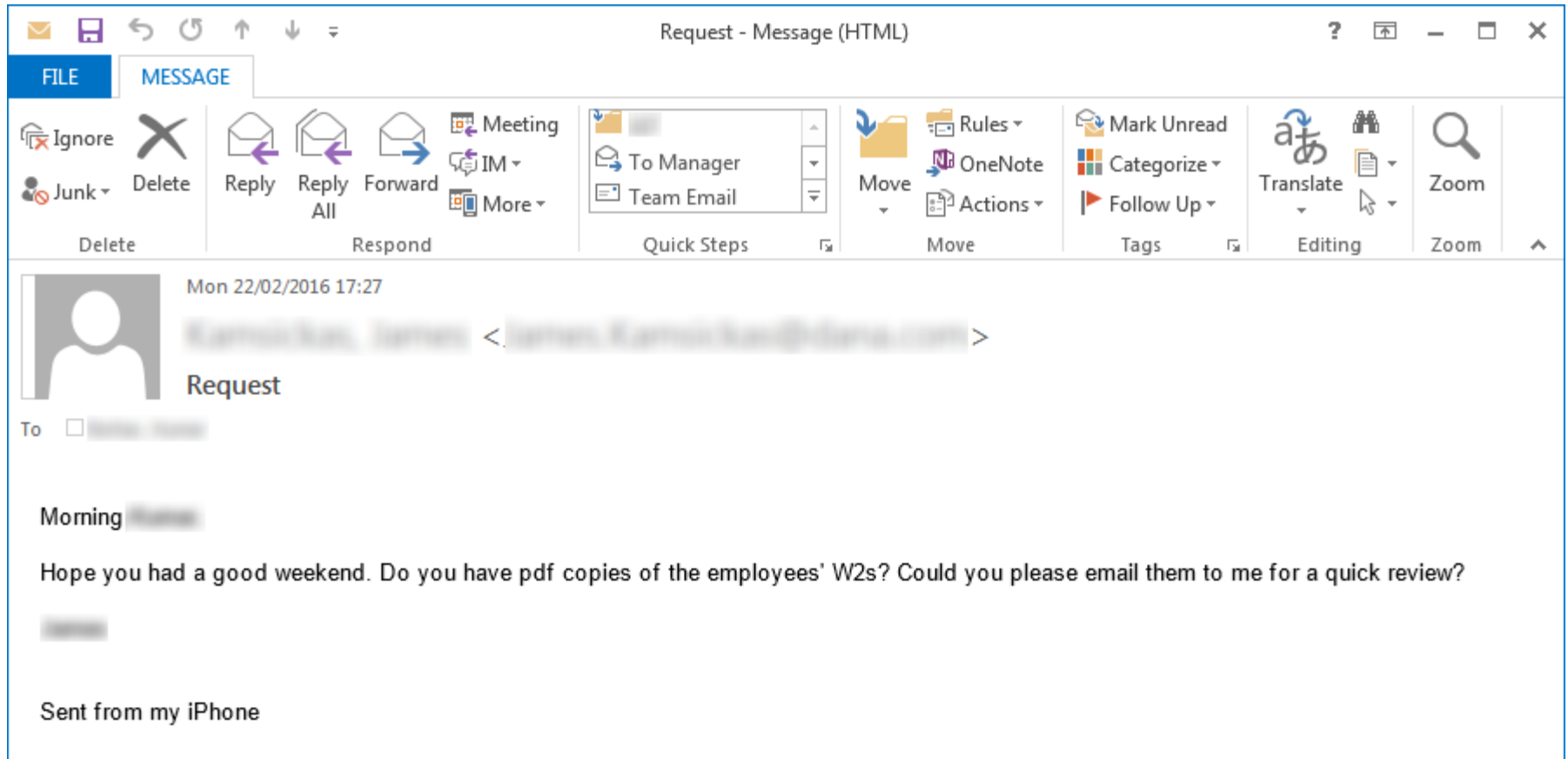
Government Agencies

[U.S. Department of Justice](#)

Most Popular

- 1 5 Things You Should Never Put In A Client Email
- 2 How To Turn Nonbillable Work Into Big Bucks
- 3 3 Recent Rulings On Client Conflicts You Should Know
- 4 Panama Papers Data Dump Includes BigLaw Intermediaries

W-2 PHISHING SCAMS



WHAT DO THE LAWYERS DO?

- Assist with execution of breach response plan
- Identify legal and contractual obligations
- Identify potential insurance coverage and notify insurers
- Identify scope of the breach
- Oversee forensic investigation into incident
- Work with law enforcement
- Prepare required notifications under applicable state and federal laws



NOTICE TO REGULATORS

IC 24-4.9-2-10

"Personal information"

Sec. 10. "Personal information" means:

- (1) a Social Security number that is not encrypted or redacted;
or
- (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
 - (A) A driver's license number.
 - (B) A state identification card number.
 - (C) A credit card number.
 - (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

The term does 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.

As added by P.L.125-2006, SEC.6.

NOTICE TO REGULATORS

IC 24-4.9-2-10

"Personal information"

Sec. 10. "Personal information" means:

(1)
or
(2)
na
ar

IC 24-4.9-3-1

Disclosure of breach

Sec. 1. (a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose:

- (1) unencrypted personal information was or may have been acquired by an unauthorized person; or
- (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key;

if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-43-5-3.5), identity theft, or fraud affecting the Indiana resident.

The ter
publicl
govern
As add

NOTICE TO REGULATORS

IC 24-4.9-2-10

"Personal information"

Sec. 10. "Personal information" means:

(1)
or
(2)
na
ar

IC 24-4.9-3-1

Disclosure of breach

Sec. 1. (a) Except as provided in section 4(c), 4(d), and 4(e) of this chapter, a person who discloses information that is confidential or otherwise protected by law or contract shall be liable for damages.

thi
se
an

IC 24-4.9-4-2

Action by attorney general

Sec. 2. The attorney general may bring an action under this chapter to obtain any or all of the following:

- (1) An injunction to enjoin future violations of IC 24-4.9-3.
- (2) A civil penalty of not more than one hundred fifty thousand dollars (\$150,000) per deceptive act.
- (3) The attorney general's reasonable costs in:
 - (A) the investigation of the deceptive act; and
 - (B) maintaining the action.

As added by P.L.125-2006, SEC.6.

The ter
publicl
govern
As add

if
tha
in
ide

NOTICE TO REGULATORS



INDIANA DATA BREACH NOTIFICATION FORM

OAG Form 1079 (R1 / 09-14)

Identity Theft Unit

OFFICE OF ATTORNEY GENERAL
Consumer Protection Division
Government Center South, 5th floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 233-4393 – Fax

Name and Address of Entity or Person that owns or licenses the data subject to the breach			
Name			
Street Address		City	State
			Zip Code
Submitted by		Title	Dated
Firm Name and Address (<i>if different than entity</i>)			Telephone
Email		Relationship to Entity whose information was compromised	

NOTICE TO REGULATORS

Reason for delay, if any, in sending notification

Description of Breach (*select all that apply*)

<input type="checkbox"/> Inadvertent disclosure	<input type="checkbox"/> External system breach (e.g. hacking)
<input type="checkbox"/> Insider wrong-doing	<input type="checkbox"/> Other
<input type="checkbox"/> Loss or theft of device or media (e.g. computer, laptop, external hard drive, thumb drive, CD, tape)	

Information Acquired (*select all that apply*)

<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Name in combination with (<i>select all that apply</i>)
	<input type="checkbox"/> Driver's License Number <input type="checkbox"/> State Identification Number
	<input type="checkbox"/> Credit Card or Financial Account Information
	<input type="checkbox"/> Debit Card Number (<i>in combination with security code, access code, password or PIN for account</i>)

List dates of previous breach notifications (*within last 12 months*)

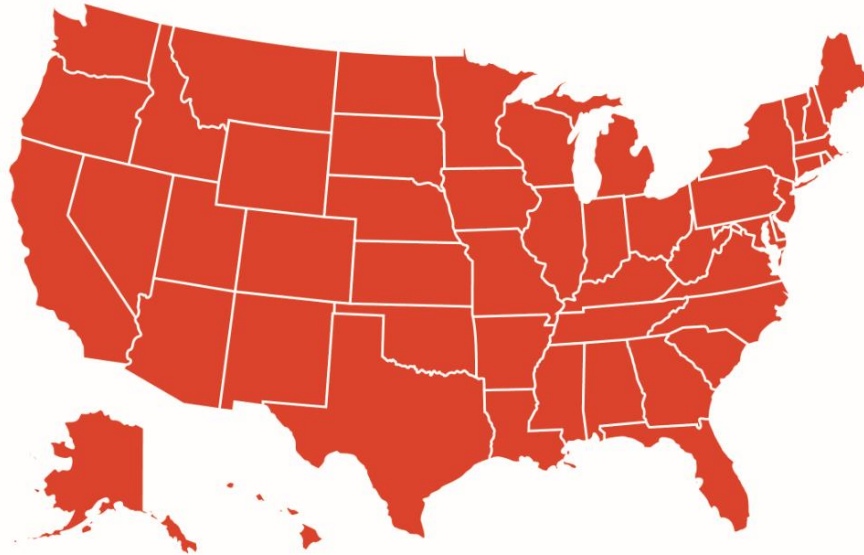
NOTICE TO REGULATORS

Since this breach, we have taken the following steps to ensure it does not reoccur *(attach additional pages if necessary)*



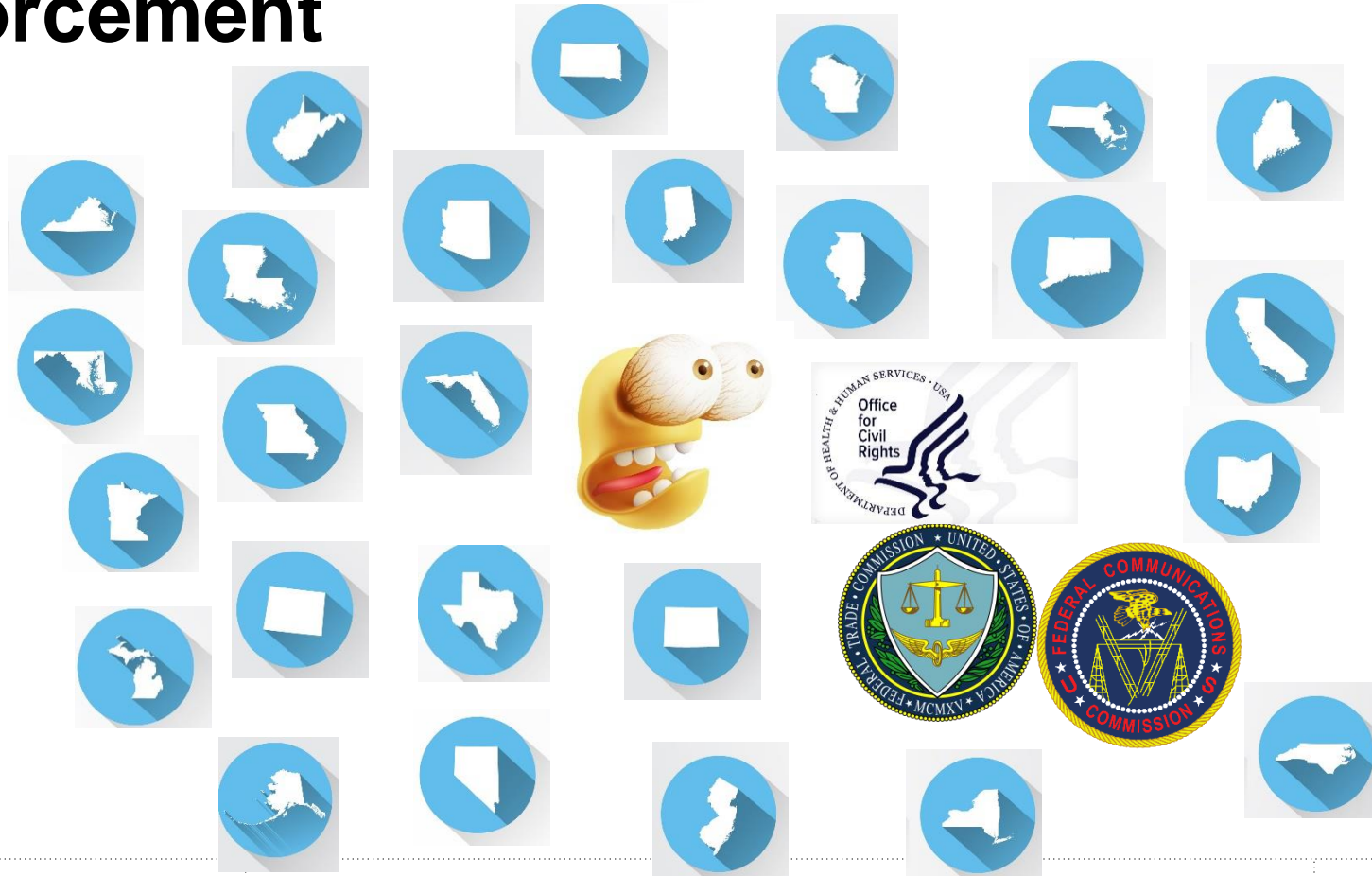
Compliance with Breach Notification Laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.





Multi-State Enforcement





What Laws are AGs Enforcing?

- Unfair and Deceptive practice laws
- Personal information protection laws
- Data breach notice laws





What Laws are AGs Enforcing?

- HITECH
- Coordination with HHS





Structure of a Multi-State Action

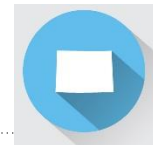
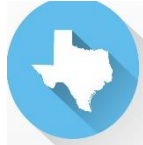
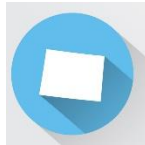
Lead states



Executive Committee



Participating states



DATA BREACH LITIGATION: CONSUMER CLASS ACTIONS

Home » Class Action » negligence » News » unjust enrichment» [Email to Friend](#)

Class action filed over Anthem data breach

November 13, 2014 1:33 PM
By JIM BOYLE

A Carbon County, Pa., man has filed a class action lawsuit in Pennsylvania against soft drink giant Coca-Cola over an estimated 70,000 people whose laptops were stolen from the company's servers.

Shane Enslin, of Albrightsville, Pa., filed the lawsuit claiming damages for the thousands of dollars in lost data by the thefts. He claims that the lawsuit represents the potential victims of the breach.

IT/NETWORKING

Maine man files \$5M class action suit over Anthem data breach

BETH BROGAN ON 3/14/2015
SOURCE: BANGOR DAILY COURIER

**available in print
brushed chrome
with custom
PLUS fast delivery**


Portland driver suing Uber over data breach

Data breach happened in May 2014, announced in February 2015
By KOIN 6 News Staff
Published: March 14, 2015, 4:30 pm

[Twitter](#) [Google+](#) [Facebook](#) [Pinterest](#)

[f | Share](#) [t | S](#)

March 06--PORTLAND, ME (AP) — A Portland driver has filed a lawsuit against Uber, claiming the company's data breach exposed his location information to hackers.



BREACH RESPONSE: IMPACT ON LITIGATION



“I know plenty of single people who look at whether someone who’s proposed to date is married or not. So if you’re not married and there’s a report out there saying you are, that’s a potential injury.”

- Justice Sotomayor, Oral Argument before U.S. Supreme Court, November 2, 2015

Spokeo, Inc. v. Robins, 578 U.S. ____ (2016)



BREACH RESPONSE: IMPACT ON LITIGATION



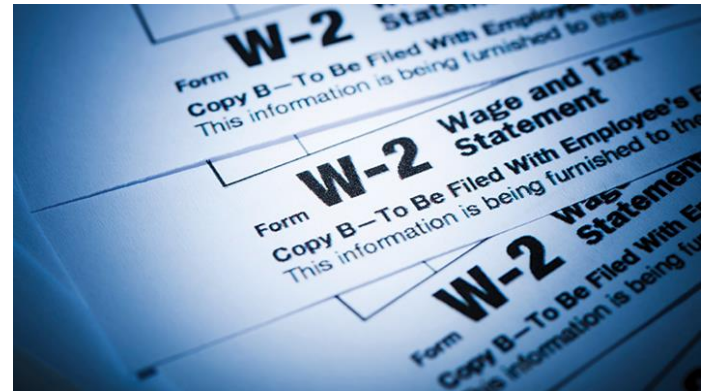
Chief Judge Diane Wood,
Oral Argument before Seventh
Circuit Court of Appeals,
January 13, 2016



Judge David Hamilton, Oral Argument
before Seventh Circuit Court of
Appeals, January 13, 2016

Lewert v. P.F. Chang's China Bistro, Inc.,
819 F.3d 963 (7th Cir. 2016)

W-2 PHISHING SCAM: IMPACT ON LITIGATION

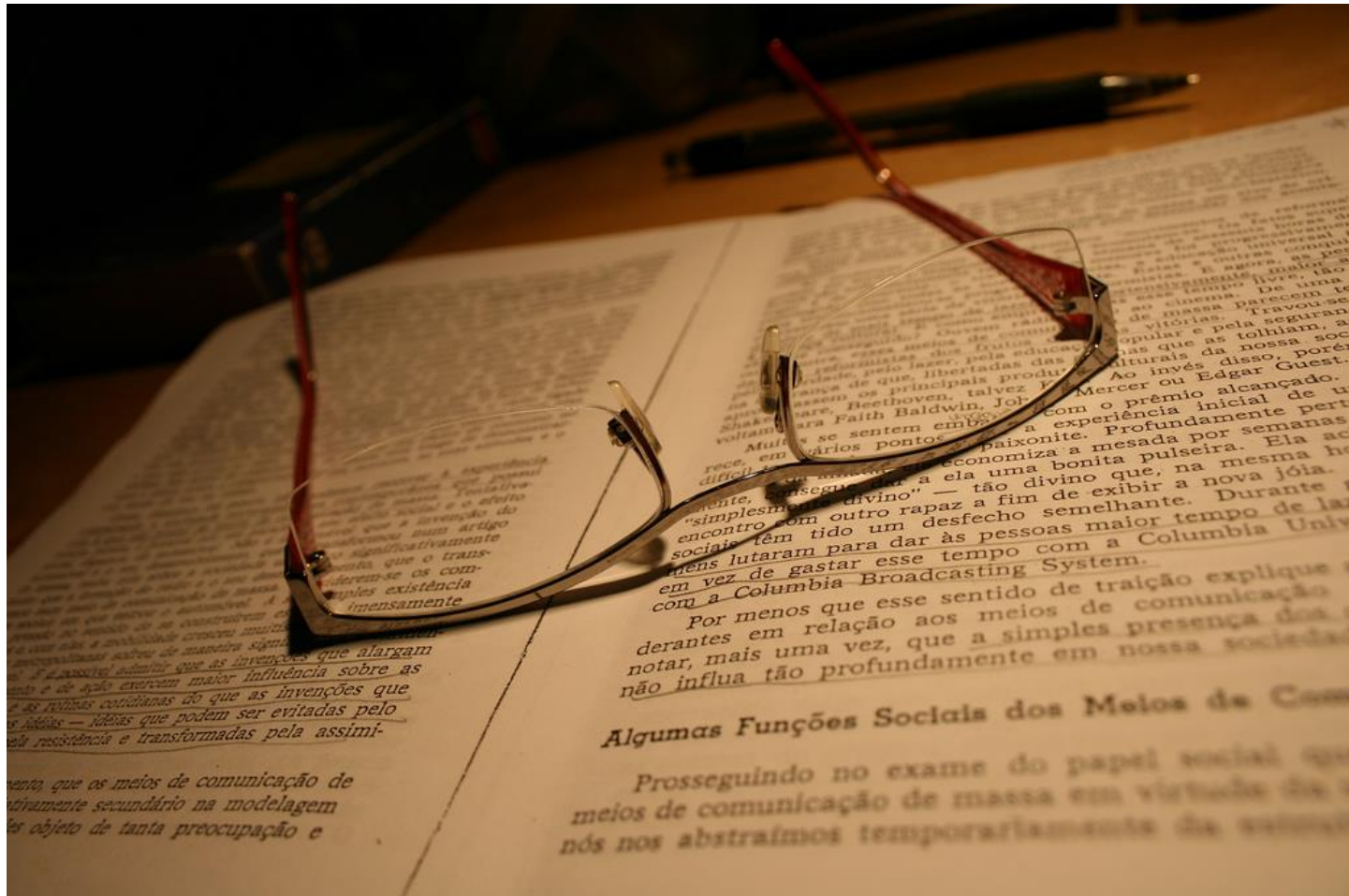


How do we all work together?

*Achieving Goals,
Preserving Privilege,
Assisting Investigation*



CASE STUDIES



GENESCO, INC. v. VISA U.S.A., INC.

GENESCO



IN RE TARGET CORP. CUSTOMER DATA SECURITY BREACH LITIGATION



BANNEKER VENTURES, LLC v. GRAHAM **(WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY)**



IN RE EXPERIAN DATA BREACH LITIGATION



KEY TAKEAWAYS

Engage Outside Counsel

- Make clear that communications are for purpose of obtaining or providing legal advice.
- Have a separate engagement letter, possibly new counsel.

Effectively Work With Regulators

- Understand regulators' role
- Consider lessons learned and mitigation
- Be mindful of deadlines

Keep Confidential

- Communications should be shared only under limited circumstances.

Questions?

Stephen Reynolds

(317) 236-2391

stephen.reynolds@icemiller.com