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
   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

From: Candidate, Joe <joe.candidate@gmail.com>
To: Joe
Subject: Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on 9/15/2013 8:44 PM

Time left 57:45:37

Next >>
MALICIOUS INSIDERS
Employee of Law Firm Wilson Sonsini Charged With Insider Trading

By MATTHEW GOLSTEIN SEPTEMBER 18, 2014 2:48 PM

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

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

Dmitry Braverman, an information technology engineer for Wilson Sonsini, was charged Tuesday for allegedly generating $297,000 in illegal profits from inside information.

Braverman, 41, was arrested by federal agents and law enforcement spokesman said.

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

By Jess Davis

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. Laouitaris, 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 Laouitaris 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, Laouitaris 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.
W-2 Phishing Scams

Request - Message (HTML)

Mon 22/02/2016 17:27

James.Kennedy@Iine.com

Request

Morning [Name]

Hope you had a good weekend. Do you have pdf copies of the employees’ W2s? Could you please email them to me for a quick review?

Sent from my iPhone
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) any information that is obtained from a person and that is maintained in a record containing personal information about the person;

(2) any other information that is acquired, generated, or maintained by any person that is linked or related to an individual.

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.
NOTICE TO REGULATORS

IC 24-4.9-2-10
"Personal information"
Sec. 10. "Personal information" means:

(1)
(2)

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, if a person is being notified of a breach of the

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.
**NOTICE TO REGULATORS**

**INDIANA DATA BREACH NOTIFICATION FORM**

OAG Form 1079 (R1 / 09-14)
Identity Theft Unit

| Name and Address of Entity or Person that owns or licenses the data subject to the breach |
|---|---|---|---|
| Name |  |

<table>
<thead>
<tr>
<th>Street Address</th>
<th>City</th>
<th>State</th>
<th>Zip Code</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Submitted by</th>
<th>Title</th>
<th>Dated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firm Name and Address (if different than entity)</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email</th>
<th>Relationship to Entity whose information was compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# NOTICE TO REGULATORS

**Reason for delay, if any, in sending notification**

________________________________________

**Description of Breach (select all that apply)**

- [ ] Inadvertent disclosure
- [ ] Insider wrong-doing
- [ ] Loss or theft of device or media (e.g. computer, laptop, external hard drive, thumb drive, CD, tape)
- [ ] External system breach (e.g. hacking)
- [ ] Other

**Information Acquired (select all that apply)**

- [ ] Social Security Number
- [ ] Name in combination with (select all that apply)
  - [ ] Driver’s License Number
  - [ ] State Identification Number
  - [ ] Credit Card or Financial Account Information
  - [ ] Debit Card Number (in combination with security code, access code, password or PIN for account)

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

<table>
<thead>
<tr>
<th>Date 1</th>
<th>Date 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

Class action filed just days after Anthem breach

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

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
“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

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.
IN RE TARGET CORP. CUSTOMER DATA SECURITY BREACH LITIGATION

TARGET

IceMiller® LEGAL COUNSEL

icemiller.com
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