Cyber Security &
Data Breach for Mediators

MAKE IT MATTER
Promoting Mediator Professionalism

26th Annual Conference
Florida Dispute Resolution Center

August 9–11, 2018
JW Marriott, Grande Lakes Orlando

McDonald Hopkins LLC
Attorneys at Law

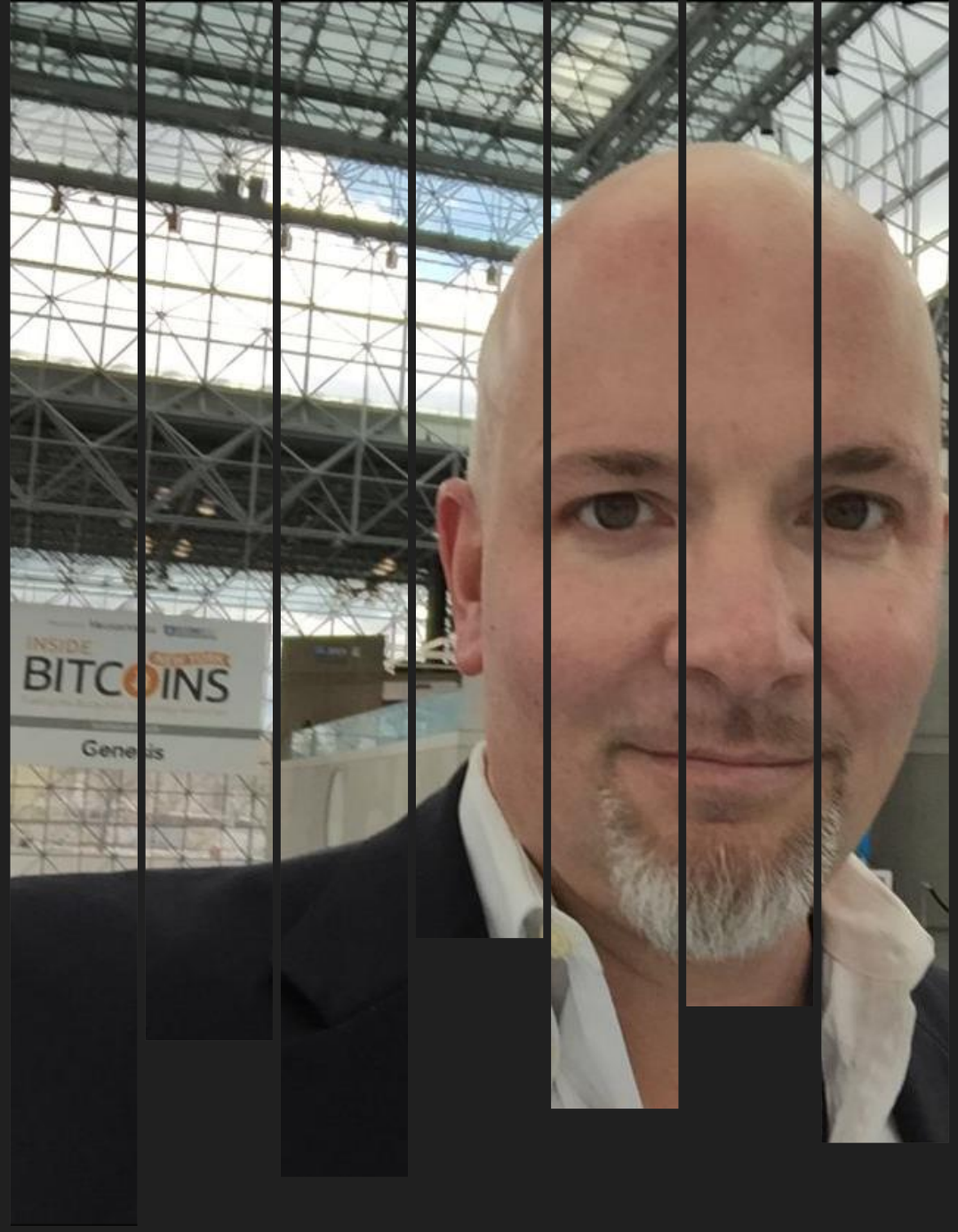
chopkins@mcdonaldhopkins.com

Christopher Hopkins

McDonald Hopkins LLC – West Palm Beach

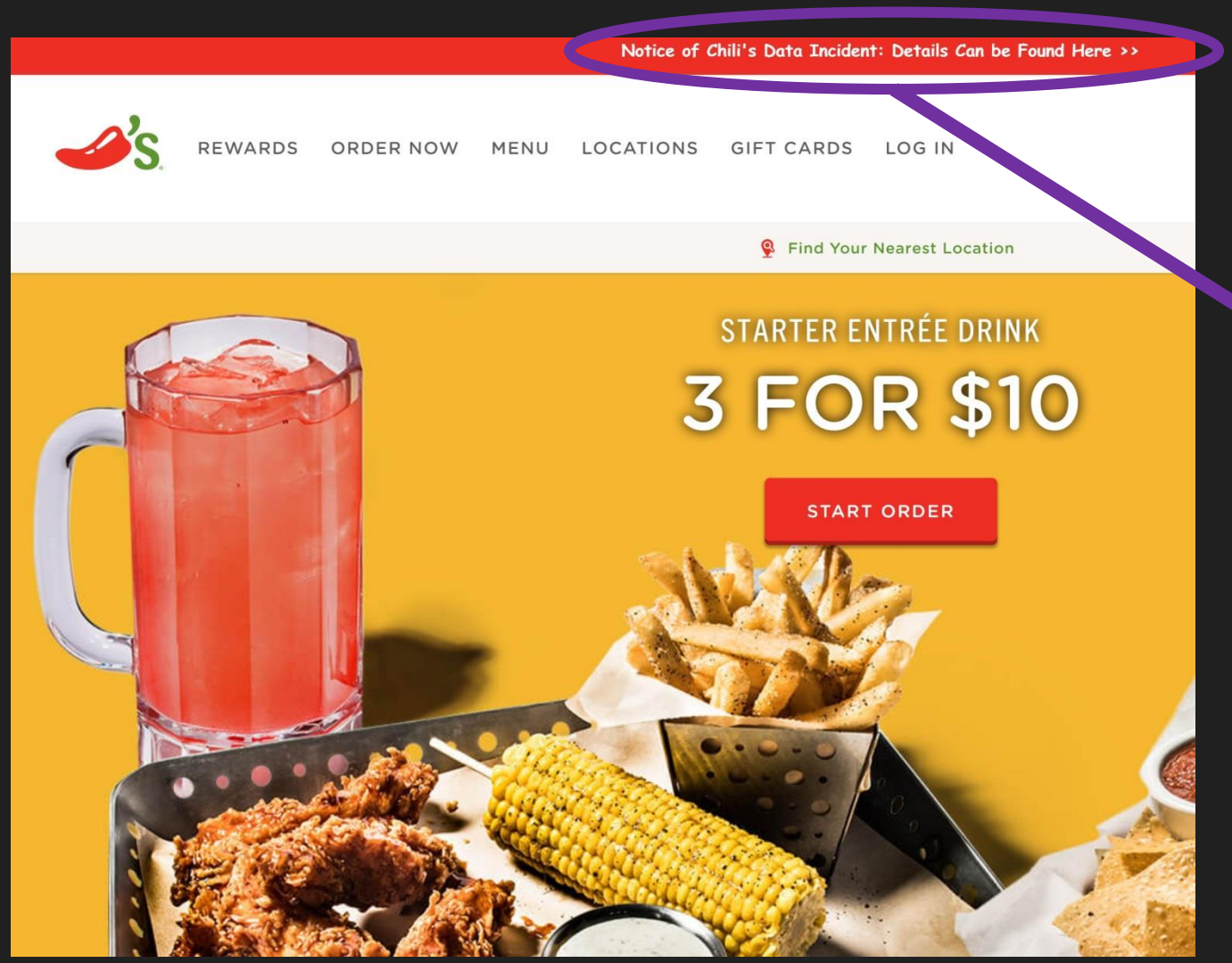
Lawyer, mediator, and arbitrator.

Christopher's practice involves a wide range of emerging technologies including cyber security, internet crimes, policy drafting, privacy, and social media discovery.



I Want My Baby Hack, Baby Hack, Baby Hack

McDonald Hopkins



NEWS RELEASES

NOTICE OF UNAUTHORIZED ACCESS TO CHILI'S® GRILL & BAR GUEST DATA

Dear Valued Guests,

This notice is to make you aware that some Chili's restaurants have been impacted by a data incident, which may have resulted in unauthorized access or acquisition of your payment card data, and to provide you information on steps you can take to protect yourself and minimize the possibility of misuse of your information.

What is Data Breach?

What is a DATA BREACH?

McDonald Hopkins

Definition: "A **data breach** is a security incident in which sensitive, protected or confidential **data** is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so."

Data breach - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/**Data_breach** Wikipedia

More about Data breach

About this result • Feedback

What are Hackers Trying to Steal?

PII

Personally Identifiable Information PII

FIRST name + LAST name +

Social, driver's license, credit card number, banking info, DOB, email and user names, security questions/answers, and biometrics (anything that leads to $$$)

PHI

Protected Health Information PHI

Medical records, health status, provision of health care, payment for health care

$$

Money & Account Information

Account information. Ransomware.

ELEMENTS OF

Negligence

The same framework for "ordinary" negligence typically applies to data breach cases.

DUTY

Obligation requiring defendant to conform to a certain standard of conduct for the protection of others [plaintiff] against unreasonable risks.

BREACH

Failure to meet that duty.

CAUSATION

The defendant's breach of duty is the legal cause of damages

DAMAGES

As a result of the defendant's breach, the plaintiff suffered monetary loss.

Knight v. Merhige (Fla. 4th DCA 2014).

It's basic NEGLIGENCE theory

McDonald Hopkins

Technology Corner

The Government Can Sue Your Company for Negligent Cybersecurity

by Christopher B. Hopkins

While the risk of hackers dawned on many corporate lawyers after Target's data breach in 2013, the federal government has been actively suing corporations into cybersecurity compliance since 2005. Specifically, the Federal Trade Commission (FTC) has sued more than 50 companies for poor cybersecurity despite the lack of any specific statute on point. Even the Federal Communications Commission (FCC) has sued regulated companies for their lackluster data standards. It is not just credit card or health care data which needs to be protected, as evidenced by the recent Ashley Madison hack. All corporations need to be aware that they can be sued by injured parties (see the Seventh Circuit's *Remijas v. Neiman Marcus* opinion) as well as the federal government for what is best described as "negligent cybersecurity." The recent Third Circuit opinion in *FTC v. Wyndham* gives guidance on data practices to follow or avoid.

In April 2008, hackers broke into a Phoenix-area hotel's network and then connected to Wyndham's larger network. Using pure guesswork, the hackers paired usernames with frequently-used passwords as a brute-force method to break in. From there, hackers discovered unencrypted payment information and that Wyndam's system was practically unmonitored. Hackers repeatedly breached Wyndham's system

In *Wyndham*, the defendant was sued for failing to take these steps:

- Use firewalls at critical network points;
- Restrict access to certain IP addresses;
- Use encryption for certain customer files (not plain text);
- Monitor network for previously-discovered malware;
- Employ common protection which prevents users from selecting weak passwords;
- Employ reasonable methods to detect and prevent unauthorized access.

Along these lines, in 2007, the FTC published a guidebook, *Protecting Personal Information: A Guide for Business*, which provides these recommendations:

- Check software vendors' sites regularly for patches and alerts about new vulnerabilities;
- Set firewall controls to limit access only to trusted employees with a legitimate business purpose;
- Require employees to use strong passwords;
- Implement a data breach response plan which includes immediate investigation and steps to close off vulnerabilities.

Until the *Wyndham* case, most companies settled with the FTC which limited the amount of attention paid to the FTC's

Who is Filing Lawsuits For Data Breach?

U

Individuals

Average person who discovers that the PII, PHI or $$ has been taken due to a data breach.

V

Companies Suing Vendors Who Lost Data

A company may discover that there has been a data breach because a vendor lost the data – credit card processor, copy company, storage facility, temp company or any third party who could/should safeguard the data.

IT

Companies Suing IT Companies

If a company's computers, network, or cloud was hacked, they can sue the companies who set up / maintain the network and/or host the data.

McDonald Hopkins

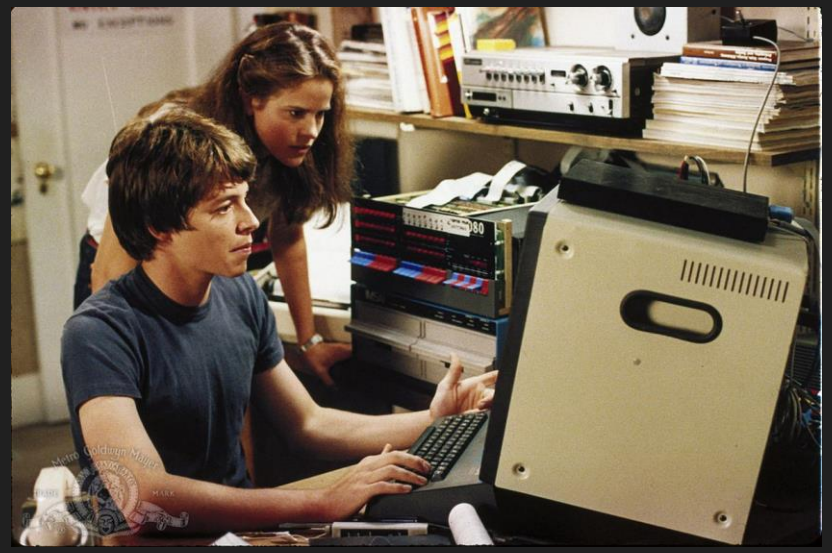
Ways To Get Hacked

*(Important information to know, both to mediate these cases **and to avoid being a victim**)*

Ways to get HACKED

McDonald Hopkins

Brute Force: In the 1983 thriller WarGames, young Matthew Broderick sets up his modem to dial every phone number in Sunnyvale, California hoping to find a way to access a game developer's system. Instead, he hits upon WOPAR, a government supercomputer. Broderick's dauntless "war dialing" is a form of brute force attack where a hacker repeatedly tries combinations to hack passwords or otherwise obtain access to an account.



Ways to get HACKED

McDonald Hopkins

Reverse Brute Force: Instead of testing a number of passwords on one account, "reverse" brute force involves testing one or just a few passwords across multiple accounts. In the wake of large hacks, long lists of widely used passwords are available online. A hacker who tries "123456" or "password" against several hundred usernames is bound to get lucky.

Ways to get HACKED

McDonald Hopkins

Social Engineering: Sometimes it does not always require coding skills to fool people into revealing information. Aside from posing as a government officer or company representative, hackers can even use social media to befriend and interact with people who might be easily fooled into disclosing information. One barebones example of social engineering revolves around testing spouse and pet names from a Facebook profile as that person's password.

Zeljka Zorz, Managing Editor
January 22, 2018

Share this article

British teenager hacked top ranking US officials using social engineering

Upcoming live webinar: "6 Steps to Successful Application Control Deployment"

How did British teenager Kane Gamble, who at the time was only 15 years old, manage to break into email accounts of the CIA and DNI chiefs, as well as gain access to a number of sensitive databases and plans for intelligence operations in Afghanistan and Iran?

The answer is social engineering.

Ways to get HACKED

McDonald Hopkins

Malware / worms: Malware is a secret code which a user unknowingly downloads and installs which, in turn, begins spying or causing damage. Malware can be as simple as code which quietly runs a script after a user clicks a link or it can be more widespread, such as when malware is furtively "baked" into commercial software. Recent examples reportedly include Staples, Sony (recall the film, The Interview) and the Stuxnet attack which plagued nuclear reactors in Iran.

Ways to get HACKED

McDonald Hopkins

Distributed Denial of Service: If you try to log into an account several times, at some point, the system will lock you out. Imagine now that hackers bombard a website with thousands of login attempts which intentionally fail and, at some point, overload the website which prevents everyone from access. That is a denial of service attack. Hackers then use multiple IP addresses to avoid being blocked (that's the "distributed" part of the hack). At a higher level, more sophisticated attacks can coax the beleaguered website to cough up data.

GOVERNMENT

Two Democratic campaigns hit with DDoS attacks in recent months

Over 50% increase in DDoS attacks recorded in Q1 2018: Verisign

More than 65 per cent of customers who experienced DDoS attacks in Q1 of this year were targeted multiple times, report said.

IANS | July 02, 2018, 18:10 IST

Ways to get HACKED

McDonald Hopkins

Phishing: A hacker may fool users into thinking that a fake website is real so that the hacker can steal usernames, passwords, and other information. The unwitting user typically hits a link upon receiving an email which insists that "you must change your password." This tricks the person into interacting with a fake version of a bank, social media, or shopping website. The fake website may also inject malware which further exploits the user's mistake. The "celeb-gate" incident in 2014, where nude celebrity cell phone images were spread across the internet, was caused by a widespread phishing scam.

ars TECHNICA

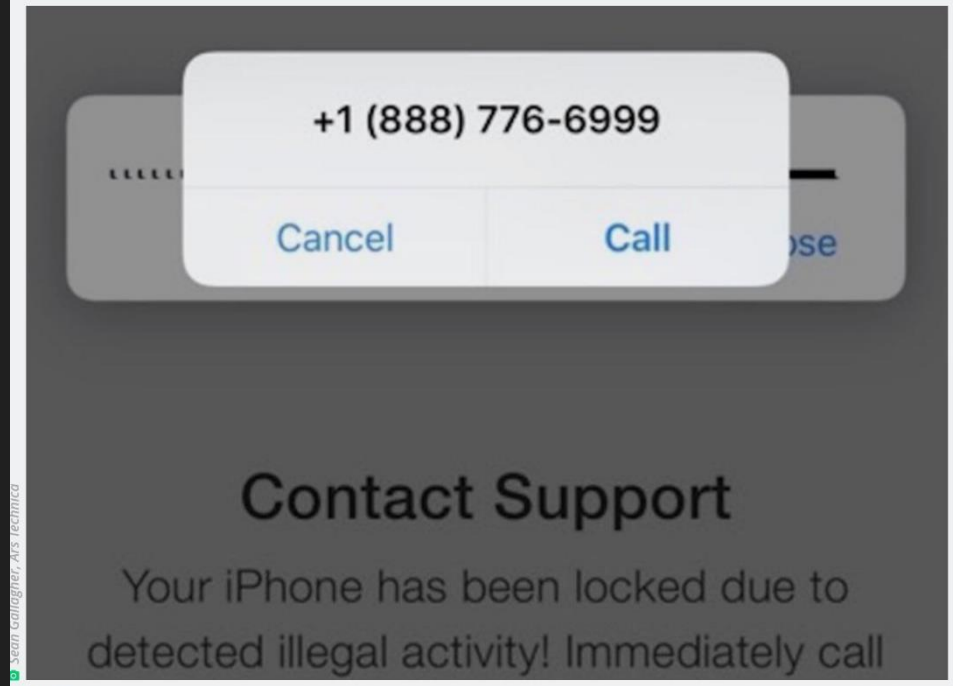
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FO

YOU RANG? —

Click on this iOS phishing scam and you'll be connected to "Apple Care"

Scam website launched phone call, connected victims to "Lance Roger at Apple Care."

SEAN GALLAGHER - 7/30/2018, 11:15 AM



Sean Gallagher, Ars Technica

Enlarge / This pop-up launches from an Apple support phishing site discovered this weekend by Ars.

Ways to get HACKED

McDonald Hopkins

Physical Access: You can probably name a few infamous hackers such as Snowden, Manning, and Anonymous. But what is the name of the cleaning service company which enters your office every night? Hacking is not just virtual. Physical access – where a hacker gets direct access to your computer – remains the most convenient way to steal data. These are often "inside jobs." This includes installing keyloggers (devices which record your keystrokes) which function like credit card skimmers on ATMs and gas pumps.

Ways to get HACKED

McDonald Hopkins

USA TODAY

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 77° INVESTIGATIONS CROSSWORDS VIDEO GRATEFUL SUBSCRIBE MORE

12 Russian intelligence officers indicted for hacking into DNC, Clinton campaign

Kevin Johnson,Erin Kelly and Jessica Estepa, USA TODAY Published 12:07 p.m. ET July 13, 2018 | Updated 4:01 p.m. ET July 13, 2018

Case 1:18-cr-00215-ABJ Document 1 Filed 07/13/18 Page 1 of 29

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	•	
	•	CRIMINAL NO.
v.	•	
	•	(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.)
VIKTOR BORISOVICH NETYKSHO,	•	
BORIS ALEKSEYEVICH ANTONOV,	•	
DMITRIY SERGEYEVICH BADIN,	•	
IVAN SERGEYEVICH YERMAKOV,	•	
ALEKSEY VIKTOROVICH LUKASHEV,	•	
SERGEY ALEKSANDROVICH MORGACHEV,	•	
NIKOLAY YURYEVICH KOZACHEK,	•	
PAVEL VYACHESLAVOVICH YERSHOV,	•	
ARTEM ANDREYEVICH MALYSHEV,	•	
ALEKSANDR VLADIMIROVICH OSADCHUK,	•	
ALEKSEY ALEKSANDROVICH POTEMKIN, and	•	
ANATOLIY SERGEYEVICH KOVALEV,	•	
Defendants.	•	

****

INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had

A Brief History of Data Breach Litigation: Standing

Who is This?

McDonald Hopkins

Snowden Revelations June 5, 2013

McDonald Hopkins

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- Read the Verizon court order in full here
- Obama administration justifies surveillance

Glenn Greenwald
The Guardian, Wednesday 5 June 2013

Snowden Revelations June 5, 2013

McDonald Hopkins

NSA Prism program taps in to user data of Apple, Google and others

- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007

- Obama orders US to draw up overseas target list for cyber-attacks

Glenn Greenwald and **Ewen MacAskill**
The Guardian, Thursday 6 June 2013

Snowden Revelations June 5, 2013

McDonald Hopkins

The XKeyscore program also allows an analyst to learn the IP addresses of every person who visits any website the analyst specifies.

1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

Search: HTTP Activity

Query Name: HTTP_in_Sweden

Justification: SwedishExtremistwebsite visitors

Additional Justification:

Miranda Number:

Datetime: 1 Week Start: 2009-01-20

HTTP Type:

Host: *alhisbah.com

Scroll down to enter a country code (Sweden is selected

Country: SE Either

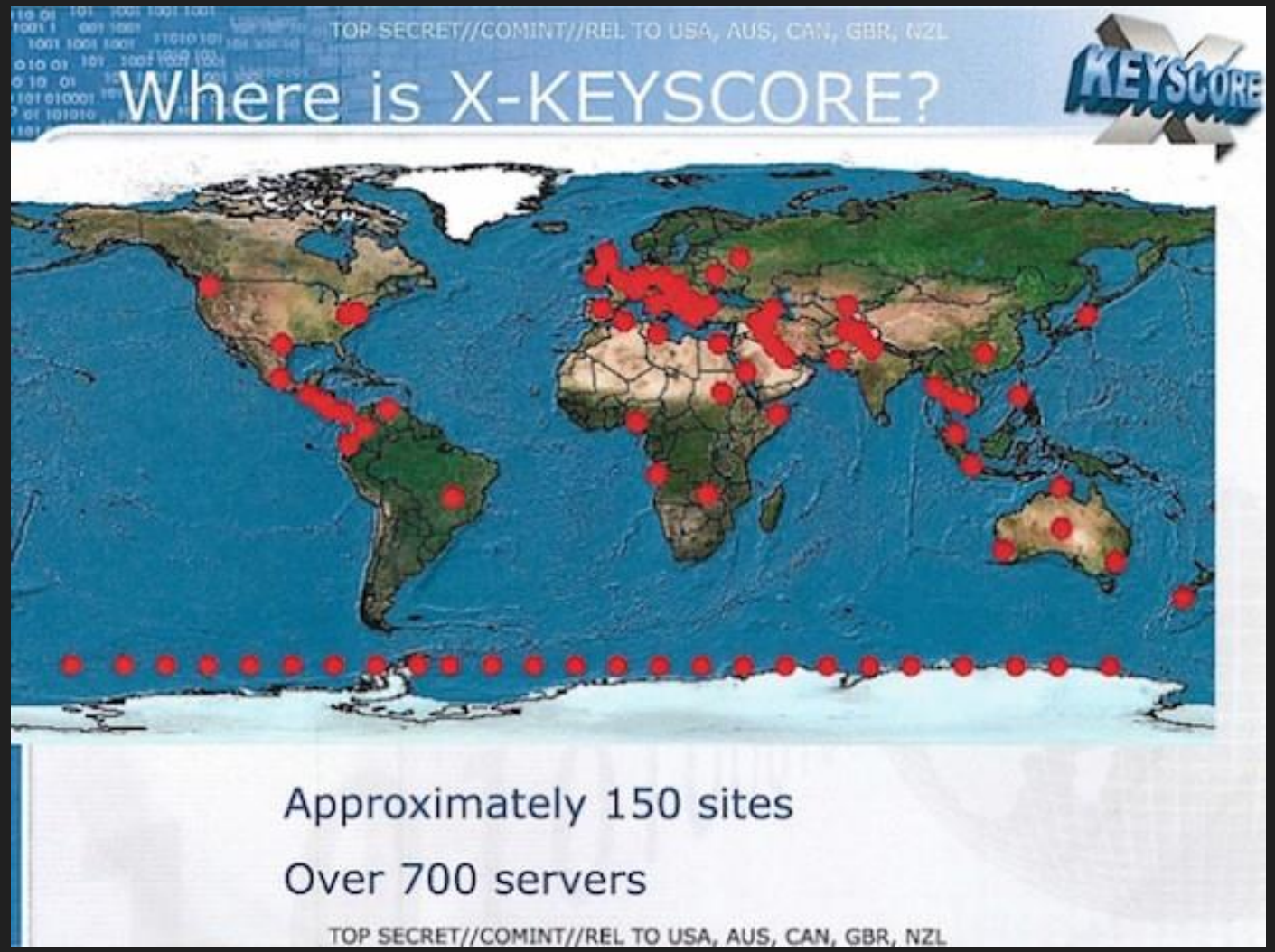
Country: To

The website URL (aka "host) is entered in with a wildcard to account for "www" and "mail" other hosts.

To comply with USSID-18 you must AND that with some other information like an IP or country

Snowden Revelations June 5, 2013

McDonald Hopkins



Snowden Revelations June 5, 2013

McDonald Hopkins

XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

- XKeyscore gives 'widest-reaching' collection of online data
- NSA analysts require no prior authorization for searches
- Sweeps up emails, social media activity and browsing history
- NSA's XKeyscore program – read one of the presentations

Glenn Greenwald
theguardian.com, Wednesday 31 July 2013 08.56 EDT

But that was June 2013

Three Months Before The Snowden Revelations

McDonald Hopkins

SUPREME COURT OF THE UNITED STATES

Syllabus

CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE, ET AL. *v.* AMNESTY INTERNATIONAL USA ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

No. 11–1025. Argued October 29, 2012—Decided February 26, 2013

Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U. S. C. §1881a, added by the FISA Amendments Act of 2008, permits the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not "United States persons" and are reasonably believed to be located outside the United States. Before doing so, the Attorney General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court's (FISC) approval. Surveillance under §1881a is

Three Months Before The Snowden Revelations

McDonald Hopkins

298. Furthermore, respondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U. S. persons with whom they communicate; (2) in doing so, the Gov-

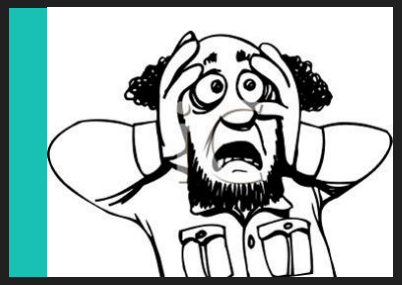
Clapper v. Amnesty International

SCOTUS – Feb 26, 2013

FISA Amendments allow the AG and DNI to surveil non-US persons reasonably believed to be outside the US (normally) after FISC approval.

DOESN'T SOUND SO SPECULATIVE NOW…:

1. "Highly speculative" that government will target the parties' communications
2. Petitioners have no actual knowledge of the government's targeting practices
3. Only speculate that the FISC would actually approve the surveillance
4. Unclear if government would succeed in acquiring the communications
5. Only speculate that petitioners' communications will be gathered



Clapper v Amnesty Int'l

Plaintiffs filed suit on the day the law went into effect and could not state in their suit that they were actually damaged or affected.

February 2013

Feb

June

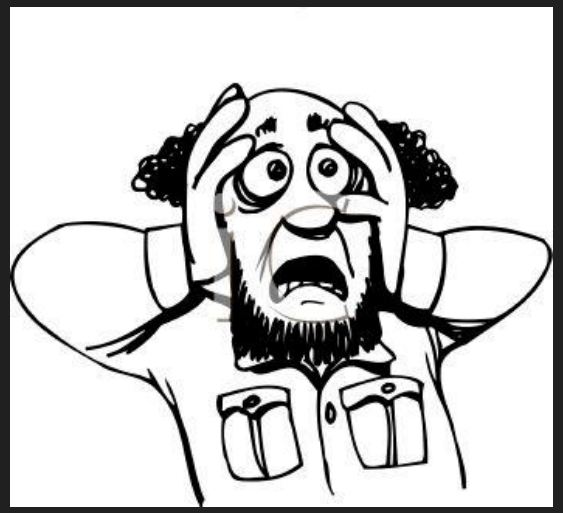
June 2013

Snowden Relevations

Revealed that <u>everyone</u> was likely affected. If the Amnesty plaintiffs had waited, they would have had their proof. But they wanted to be first to sue.

Three Months Before The Snowden Revelations

McDonald Hopkins



Wanting to Be The First Plaintiffs…

They Filed Suit Without Proof (or at least the ability to claim they were damaged).

It was too soon.

The Court held that they lacked "*standing*" to bring suit.

What Does Snowden Have to Do With Data Breach Litigation Against Private Companies?

McDonald Hopkins

No one cared about it when this case was decided.

Ironically, now this is a “landmark” precedent which is used against data breach plaintiffs.

"Snowden Lesson"

Plaintiff needs to have Article III Standing

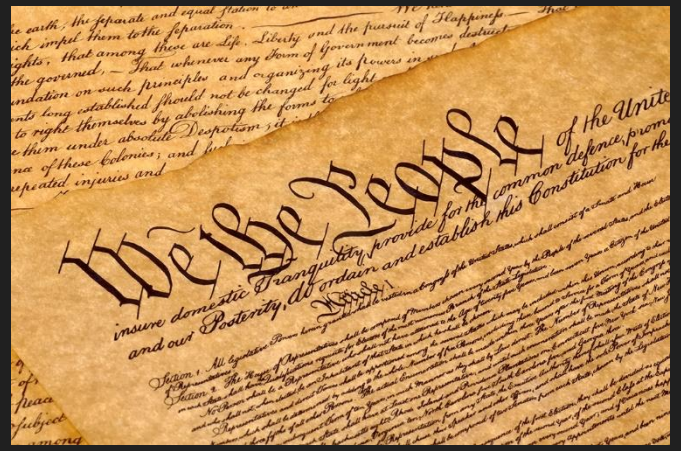
– ability to claim an actual or impending damage –

Before Filing a Lawsuit.

What is a DATA BREACH?

McDonald Hopkins

"Article III Standing"



Article 3, Section 2, Clause 1
"Case or Controversy" Clause

You have "standing" if you can allege actual or certainly impending (imminent) harm.

Three Data Breach "Standing" Cases

(this is when the parties are going to come to mediation since the future of their case is up in the air at the pleading stage…)

REMIJAS v. NEIMAN MARCUS

Seventh Circuit – July 20, 2015

ALLEGATIONS:

Neimans publically discloses a data breach of 350,000 credit card numbers. 9,200 of those credit cards were known to have been used fraudulently. No PII.

One plaintiff alleged that she had fraudulent charges on her debit card and then was the target of a scam through her cell phone.

Actual Injuries (alleged):

1. Lost time and money resolving fraudulent charges
2. Lost time and money protecting against future identity theft
3. Loss of buying from Neimans (would not have shopped there if they had known of the store's careless approach to security)
4. Lost control of personal information

Impending Injuries (alleged):

1. Risk of future fraudulent charges
2. Greater susceptibility to identify theft

REMIJAS v. NEIMAN MARCUS

Seventh Circuit – July 20, 2015

COURT:

Actual Injuries:

1. No need to speculate – 9,200 cards were used fraudulently. Other customers should not have to wait until hackers act since it is an "objectively reasonable liklelihood" that an injury would occur.

2. Already lost time and money protecting against future identity theft. This is typically NOT recoverable when the harm is not imminent. In *Clapper*, we didn't know if something had even happened. Here, Neimans admitted there was a breach.

WHALEN v. MICHAEL STORES

E.D. NY – December 28, 2015

ALLEGATIONS:

Michaels discloses a data breach of 2.6 million credit card numbers. No PII.

The lead plaintiff alleged that she had fraudulent charge on her credit card. She did not state whether it went through or if she suffered a loss.

Actual Injuries (alleged):

1. Losses arising from fraudulent withdrawals, charges and/or bank fees
2. Lost time and money protecting against future identity theft
3. Overpayment of services (would not have shopped there)
4. Lost value of credit card information

Impending Injuries (alleged):

1. Increased risk of identify theft
2. Cost associated w identity theft

WHALEN v. MICHAEL STORES

E.D. NY – December 28, 2015

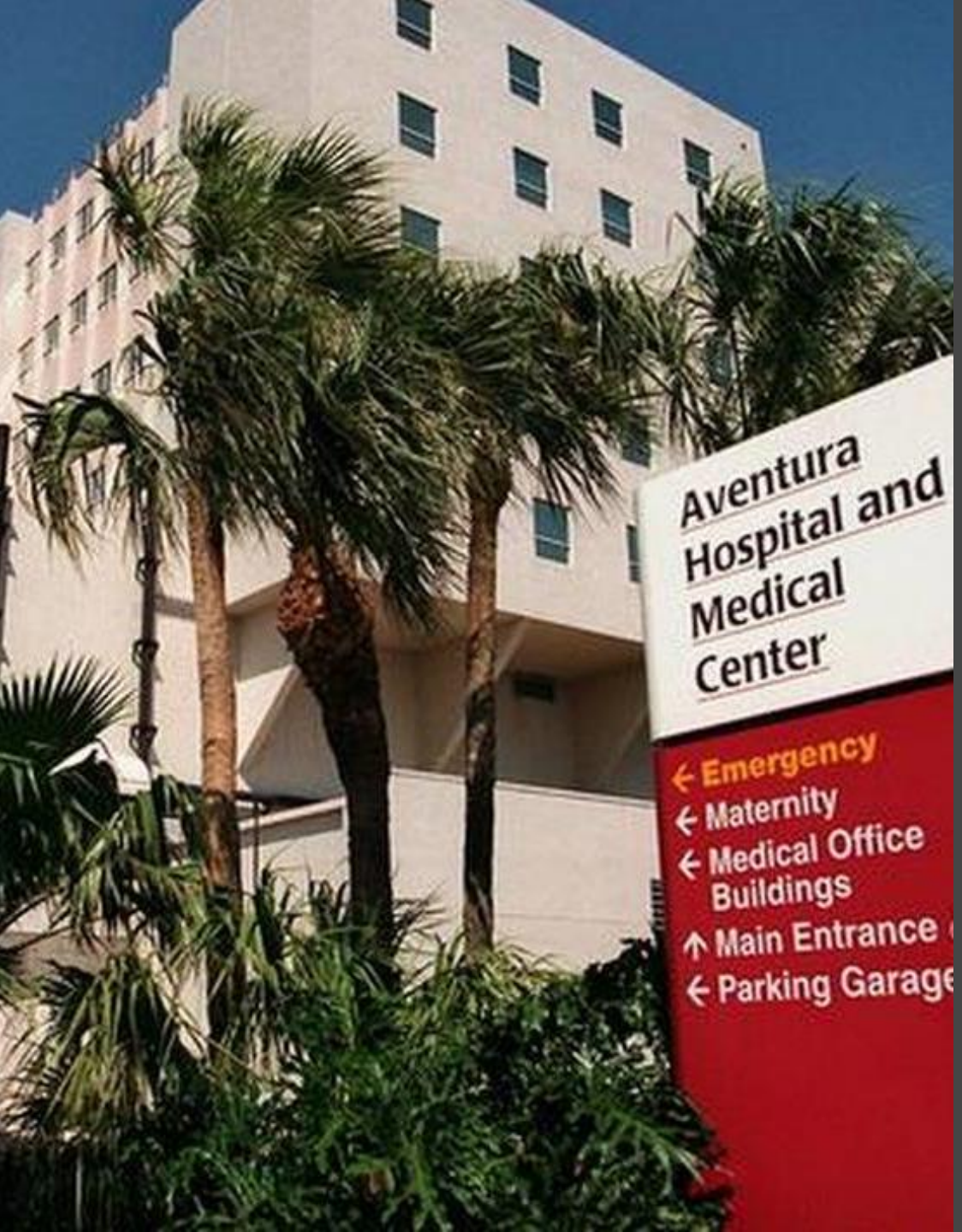
COURT:

Actual Injuries:

1. Lead plaintiff never stated that fraudulent charge was approved or she suffered a financial loss. There's a law in place re: reversing credit card charges (not debit).
2. Lost time and money protecting against future identity theft – like *Clapper*, you cannot "manufacture" standing by making an expenditure on a nonparanoid fear.
3. Overpayment of services (would not have shopped there) – conclusory. No evidence Michaels charged a different price for non-cash customers who take advantage of its security services.
4. Lost value of credit card information – no allegation how it became less valuable.

Impending Injuries:

1. Unlike Reijas, it is hard to say risk is "certainly impending." Reijas had 9200 hacked cards. Here, there are none.



Kellie Lynn Case v. Miami Beach Healthcare Group, Ltd.

S.D. Florida – February 26, 2016

ALLEGATIONS:

Hospital announced that 85,000 patient records were stolen. Former patient claims this included her personal information. She does not claim that her information was mis-used.

Actual Injuries (alleged):

1. She claims that the Hospital promised in the admission contract to protect her data. As a result, she received a diminished value of the healthcare services for which she contracted.

Kellie Lynn Case v. Miami Beach Healthcare Group, Ltd.

S.D. Florida – February 26, 2016

Court:

This identified injury – *"the difference between the price Case paid for Defendants' services as promised and the actual diminished value of her health care services"* – is not sufficiently concrete or particularized to meet this Court's jurisdictional requirements.

Anatomy of Data Breach Suit

Data Breach Litigation

McDonald Hopkins

McDonald Hopkins
A business advisory and advocacy law firm®

505 South Flagler Drive
Suite 300
West Palm Beach, FL 33401

P 561.472.2121
F 561.472.2122

Direct Dial: 1.561.847-2346
Email: chopkins@mcdonaldhopkins.com

April 3, 2018

VIA EMAIL AND FEDERAL EXPRESS
tax_advisors@att.net
Bad Person, individually
And as president of
Company Committing Data Breach, Inc.
1234 S. Flagler Drive
West Palm Beach Beach, Florida 33401

Re: Injured Parties, on behalf of themselves and
All others similarly situated adv. Bad Person, individually, and
Company Comitting Data Breach

CONFIDENTIAL, ONE-TIME SETTLEMENT DEMAND

Dear Bad Person:

It Starts With A Demand Letter

Anatomy of a Data Breach Suit

McDonald Hopkins

ACTIONS / MISTAKES AT ISSUE:

- The IT Department should not call it a “data breach.” Only counsel should confirm it is a breach. Call it an “incident.”
- Watch the clock. Most states have data breach reporting requirements.
- Watch your language! If you call it a “breach,” that could start the clock on mandatory reporting requirements.
- Defense counsel will hire forensic experts. That way their report is privileged and all communications are privileged.

Anatomy of a Data Breach Suit

McDonald Hopkins

Claims:

- Negligence
- Breach of Fiduciary Duty
- Breach of Contract
- Violation of Florida Information Protection Act
- Violation of Florida Deceptive and Unfair Trade Practice Act
- Almost always a class action…

See Attias v. Carefirst, Inc. (8th Cir. 2017)

Anatomy of a Data Breach Suit

McDonald Hopkins

Something like this:

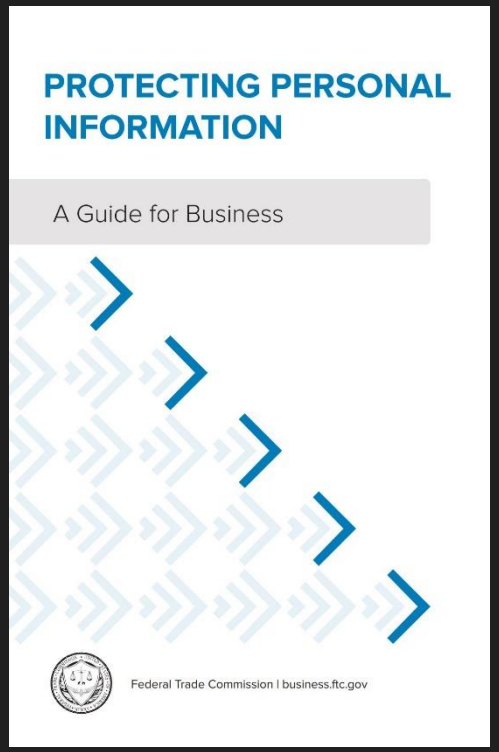
As you are aware, in May 2018, the Injured Party consulted with you and Your Company for assistance in [providing a service]. As a professional [occupation], whether handled directly by you or through Your Company, it is your sole and exclusive responsibility to secure and protect their personally identifiable information, including but not limited to their name, social security, date of birth, financial information, and bank account routing and accounts numbers (“PII”). You and Your Company failed that basic duty owed to the Injured Party and, apparently, to other clients of yours who are similarly situated.

Anatomy of a Data Breach Suit

McDonald Hopkins

Knew or Should Have Known:

- FTC can sue for "unfair or deceptive acts or practices in or affecting commerce."
- FTC claims that it is "unfair" for companies not to provide adequate cybersecurity
- It is "deceptive" not to follow your own policies
- FTC has sued more than 50 companies for cyber-negligence. This sets the standard for suits.



See FTC v. Wyndham &
Protecting Personal Information: A Guide for Business

Anatomy of a Data Breach Suit

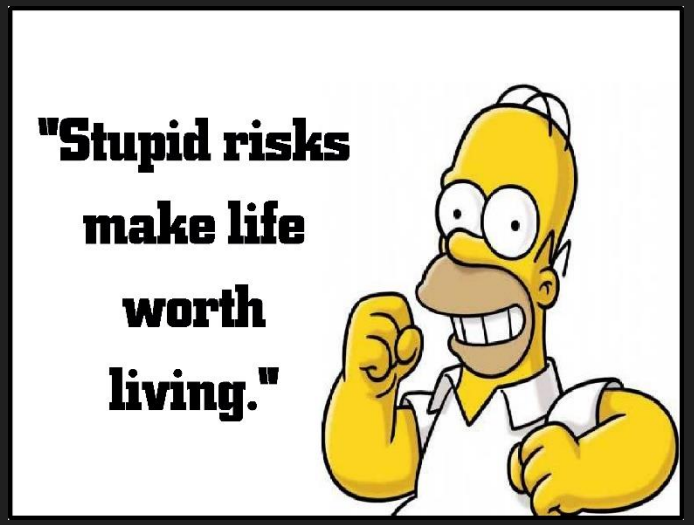
McDonald Hopkins

Knew or Should Have Known:

- Most industries have received warnings from trade associations, chambers of commerce, and regulators about industry-specific threats.

- Failure to heed those warnings will be used as evidence of negligence.

- From a demand letter:



This intrusion occurred due to Bad Company's poor security protocols, inadequate PII protection policies (if any), lack of training, and/or because of your practice of using unsecured email.

Anatomy of a Data Breach Suit

McDonald Hopkins

WHAT I TELL CORPORATE DEFENDANTS:

- Defendants should be careful with early internal emails and written communications. I tell clients: pick up the phone.
- An email to the outside world is an admission. Get counsel involved.
- Document. Get screenshots. Logs. Everything since you do not know if the hackers are going to cover their tracks.
- Do you have protocols? Were they being followed?

Anatomy of a Data Breach Suit

McDonald Hopkins

In the
United States Court of Appeals
For the Seventh Circuit

No. 17-2408

HEATHER DIEFFENBACH and SUSAN WINSTEAD,
Plaintiffs-Appellants,

v.

BARNES & NOBLE, INC.,
Defendant-Appellee.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 12 C 8617 — **Andrea R. Wood**, *Judge.*

ARGUED DECEMBER 6, 2017 — DECIDED APRIL 11, 2018

Dieffenbach v. Barnes & Noble (7th Cir. April 11, 2018)

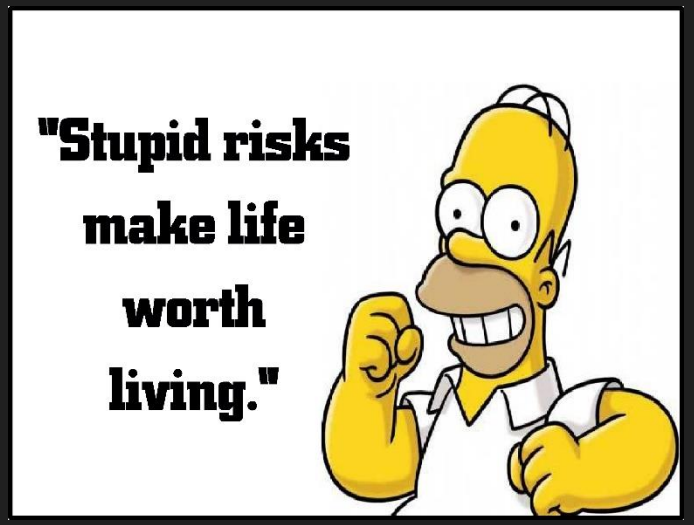
- Barnes & Noble was itself a victim!
- No state laws expressly make merchants liable for failure to "crime-proof their point-of-sales systems."
- The court stated that plaintiffs may have a difficult task showing an entitlement to collect damages from a fellow victim of the data thieves.

Anatomy of a Data Breach Suit

McDonald Hopkins

Florida Information Protection Act, F.S. 501.171:

- "Covered entity" must take "reasonable measures to protect and secure data in electronic form containing personal information."
- Provide timely and specific written notification of the breach.
- Violation of FIPA is an unfair trade practice.
- No liability under statute – but Plaintiffs can use it as a standard.
- Reporting is expensive.



Alleged Damages

What Are the Damages Plaintiffs Are Claiming?

McDonald Hopkins

In the
United States Court of Appeals
For the Seventh Circuit

No. 17-2408

HEATHER DIEFFENBACH and SUSAN WINSTEAD,
Plaintiffs-Appellants,

v.

BARNES & NOBLE, INC.,
Defendant-Appellee.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 12 C 8617 — **Andrea R. Wood**, *Judge.*

ARGUED DECEMBER 6, 2017 — DECIDED APRIL 11, 2018

Dieffenbach v. Barnes & Noble (7th Cir. April 11, 2018)

1. Temporary loss of funds while waiting for banks to reverse unauthorized charges to their accounts.

2. Monies spent on credit-monitoring services to protect the plaintiffs' financial interests.

3. The value of lost time devoted to acquiring new account numbers and notifying businesses of these changes.

What Are the Damages Plaintiffs Are Claiming?

McDonald Hopkins

Other Damages:

1. "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."

2. Lost time (a) communicating with banks, credit card companies, police; (b) from work; (c) reviewing and protecting their accounts and identity.

3. Identity Theft.

4. Future Harm (hasn't happened yet) but is "fairly traceable" to this breach. *In Re Zappos.com Customer Data Security Breach Litigation (9th Cir. March 2018).*

5. Attorney Fees and Costs.

Consider how far out into the future this can reach, especially once someone's data gets released on darkweb.

If it is only a matter of time that people are victims of data breaches, how do we know which one causes this future loss?

Companies Protecting Themselves from Liability

Data Breach Liability

McDonald Hopkins

United States Court of Appeals
For the Eighth Circuit

No. 16-3426
No. 16-3542

Matthew Kuhns, Individually and on behalf of all others similarly situated

Plaintiff - Appellant/Cross-Appellee

v.

Scottrade, Inc., a Missouri Corporation

Defendant - Appellee/Cross-Appellant

Appeals from United States District Court
for the Eastern District of Missouri - St. Louis

Submitted: April 5, 2017
Filed: August 21, 2017

Kuhn's v. Scottrade (8th Cir. 2017)

- Be careful what you promise in contracts
- Contractual obligations to protect a consumer's personally identifiable information was enough to make a claim.

Data Breach Liability

McDonald Hopkins

- Is Defendant over-promising on its website (e.g., “we are professionals devoted to the needs of individuals and businesses… we put ‘service’ back into ‘full-service’”)

- Is Defendant over-promising your security measures in Privacy Policies and Terms and Conditions?

- Did Defendant just copy your Privacy Policies and T&C from somewhere? Or leave up to website designer?

- Did Defendant train employees on risks, especially those targeting its specific industry.

- Did Defendant have up-to-date policies. Train.

- Did they have encryption? Deletion policies?

Take Away Messages About Data Breach

1

Standing

Plaintiff needs to initially allege actual damages or impending harm that is not highly speculative to survive a motion to dismiss.

2

Data Breach as Negligence

The FTC has set the standard that breaches of industry standards is actionable when it comes to cyber security. What the Defendant is doing, or is not doing, is at issue. Plaintiffs are looking at industry publications and other warnings to establish negligence.

3

Data Breach Litigation is Here To Stay

Data breaches are on the rise.

Be safe.

Christopher Hopkins

McDonald Hopkins LLC – West Palm Beach

Handouts & this PPT are at
InternetLawCommentary.com

@cbhopkins
chopkins@mcdonaldhopkins.com
Linkedin.com/in/cbhopkins