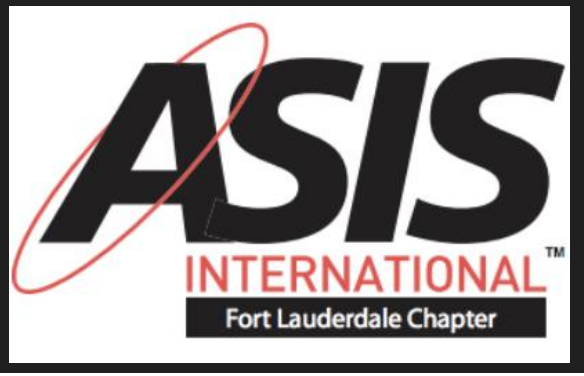
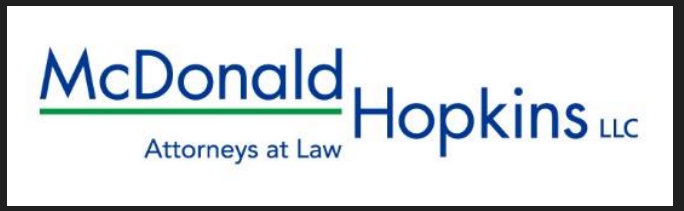



# Data Breach Litigation

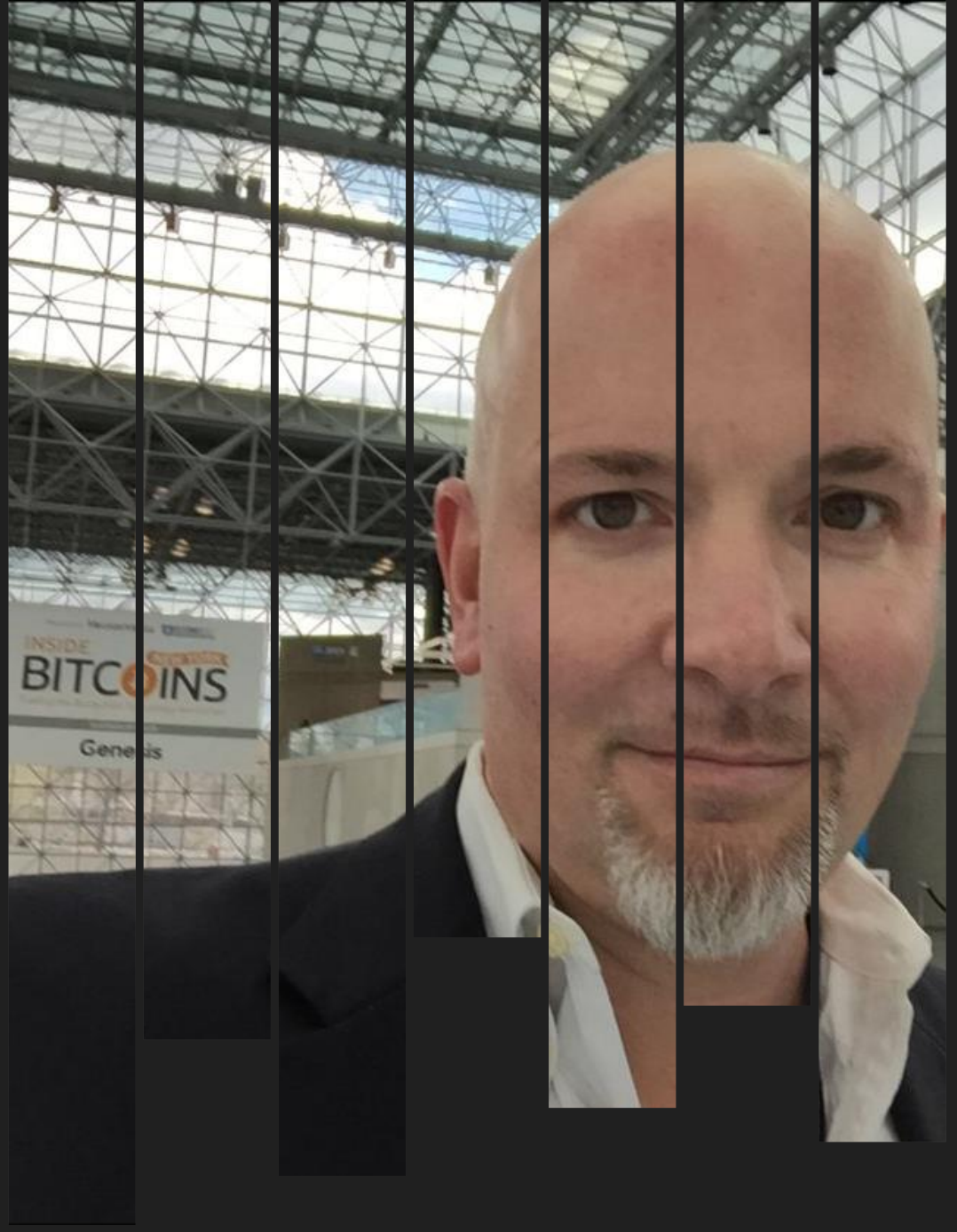
## Anatomy of a Cybersecurity Lawsuit

chopkins@mcdonaldhopkins.com

# Christopher Hopkins

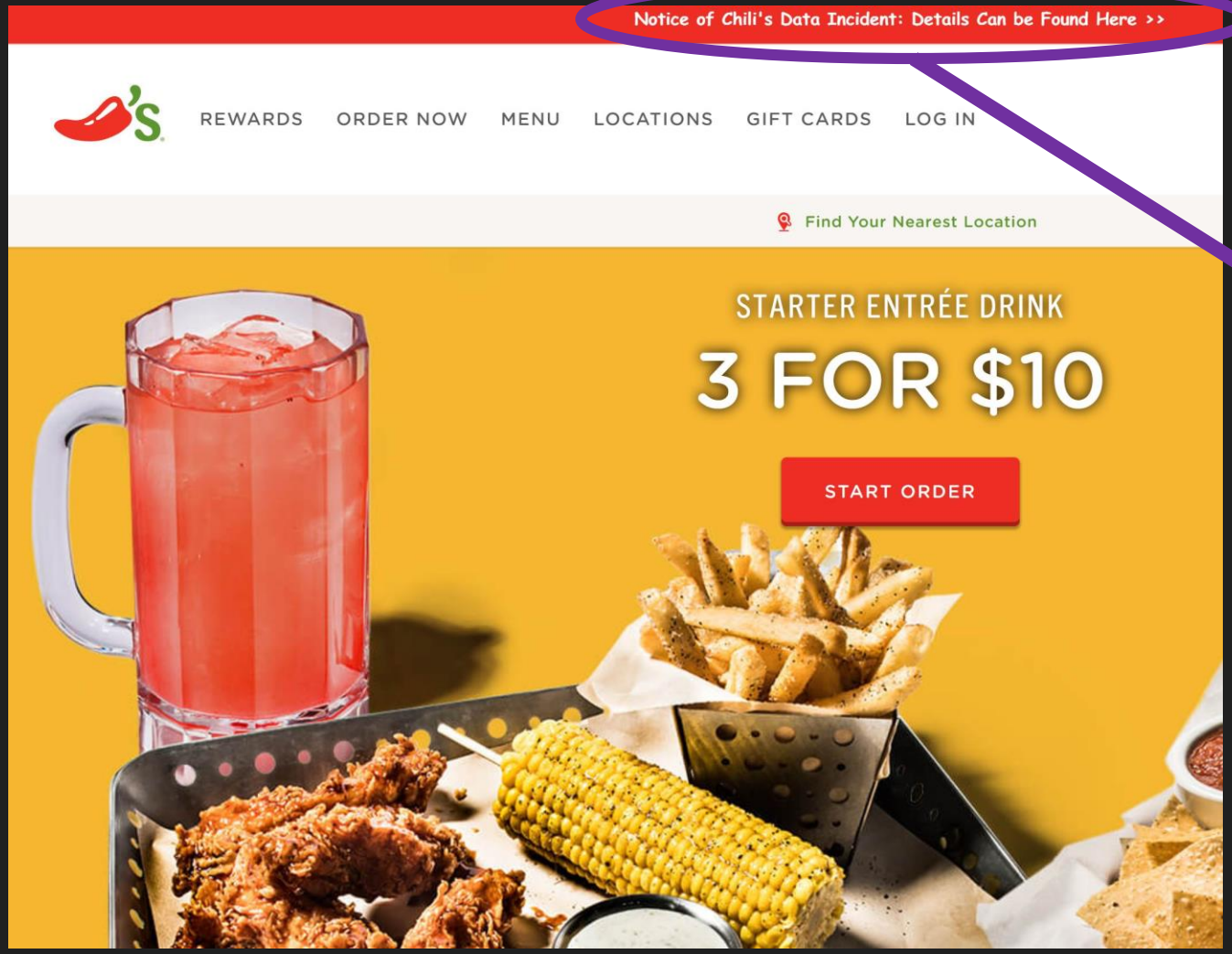
McDonald Hopkins LLC – West Palm Beach

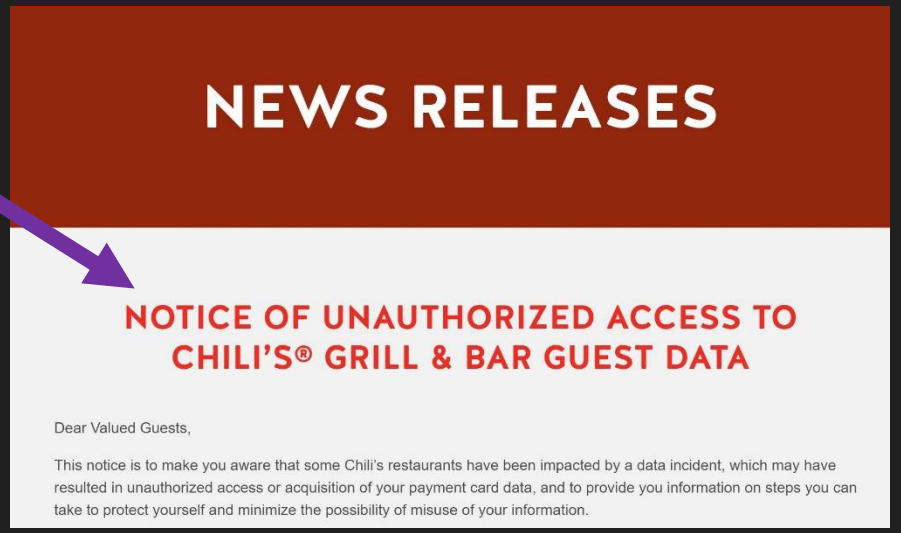
*Trial and appellate counsel with emphasis on emerging technologies: blockchain, data breach, defamation, drones, e-discovery, EULAs, internet crimes, privacy, & social media.*



# 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

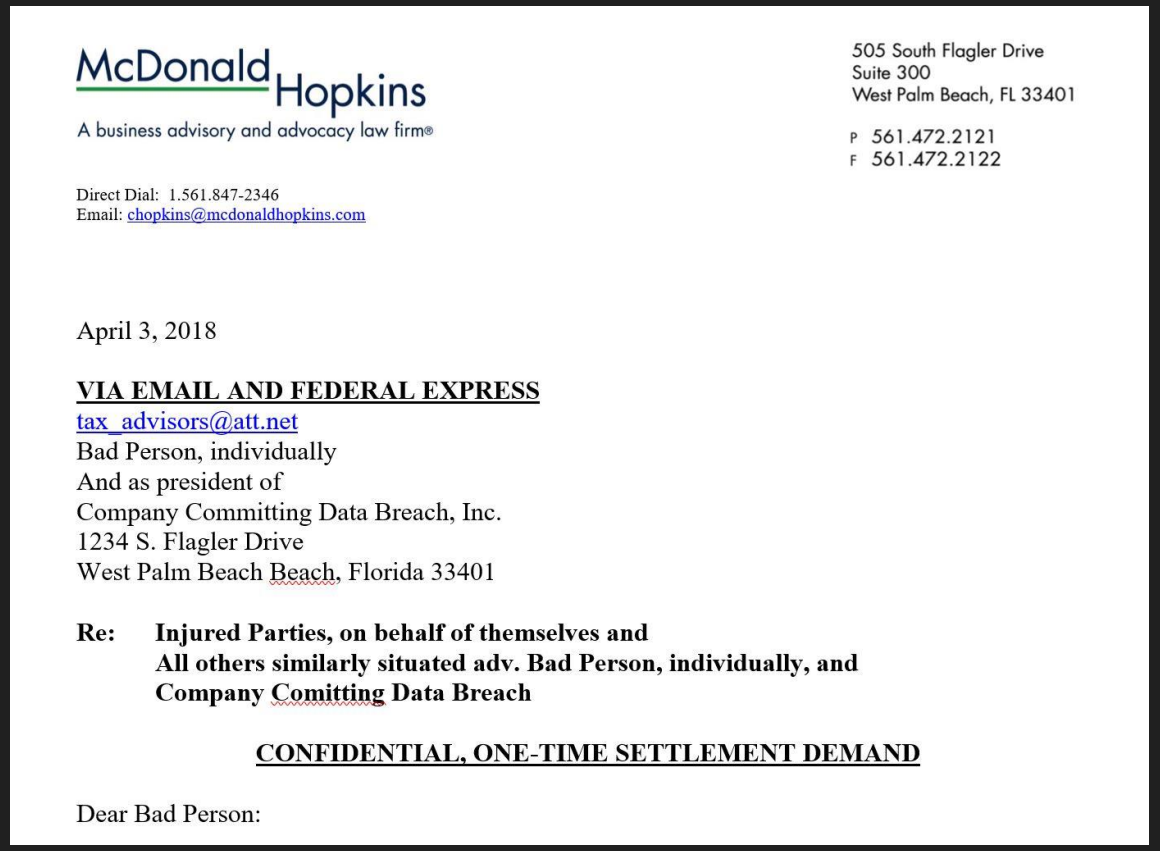
*About this result • Feedback*



# 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

## *TIPS AT THIS STAGE:*

- WATCH YOUR LANGUAGE:  not a “data breach.”  Only counsel should confirm it is a breach.  “Incident.”
- WATCH YOUR LANGUAGE #2: If you call it a “breach,” that could start the clock on mandatory reporting requirements.
- WATCH THE CLOCK.  Most states have data breach reporting requirements.
- EXPERTS: Let counsel hire forensic experts.  That way their report and communications are (more likely) privileged.

# Anatomy of a Data Breach Suit

McDonald Hopkins

## *Claims:*

- Negligence
- Breach of Fiduciary Duty
- Breach of Contract
- Florida Information Protection Act
- 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 [whatever], 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.

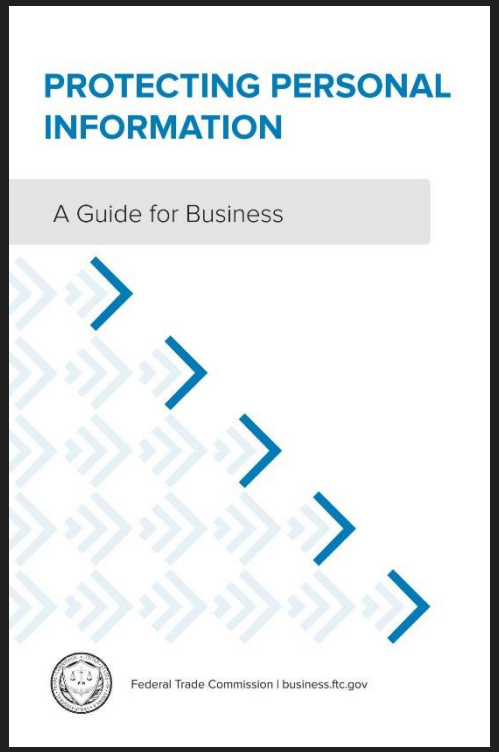
# Anatomy of a Data Breach Suit

McDonald Hopkins

*FTC SAYS YOU 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

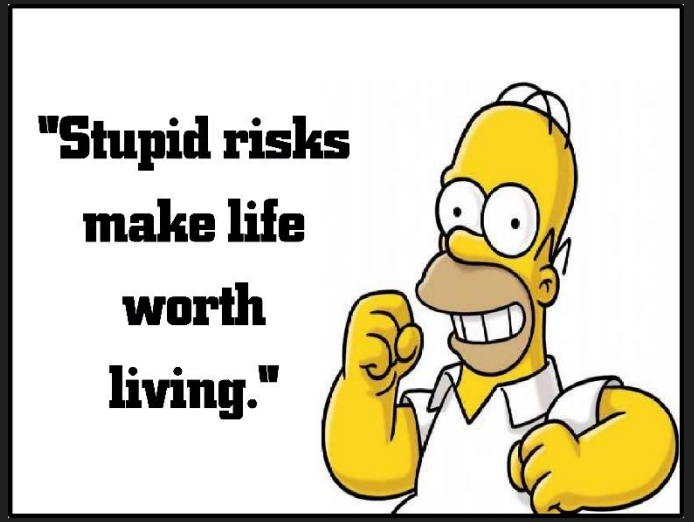
McDonald Hopkins

*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

## *TIPS AT THIS STAGE:*

- Be careful with early internal emails and written communications. 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)

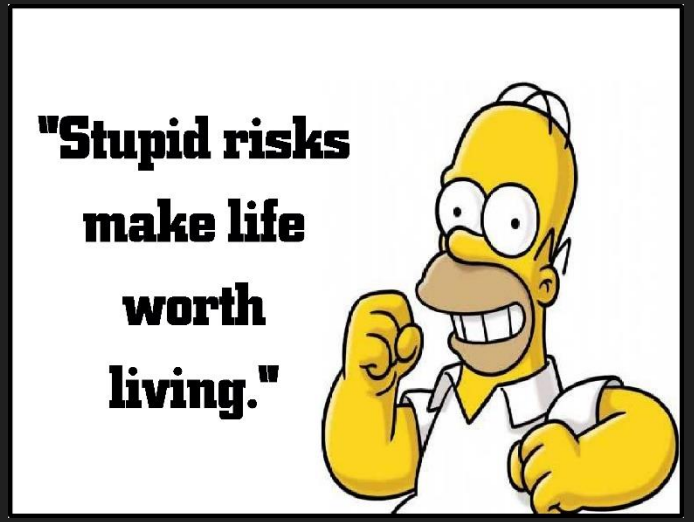
- Barnes & Noble was itself a victim!
- No state laws expressly make merchants liable for failure to "crime-proof their point-of-sales systems."
- The court stated that plaintiffs may have a difficult task showing an entitlement to collect damages from a fellow victim of the data thieves.

# 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?

Data Breach Litigation


McDonald Hopkins

# Protecting Companies From Liability

# Protect Your Company From 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*

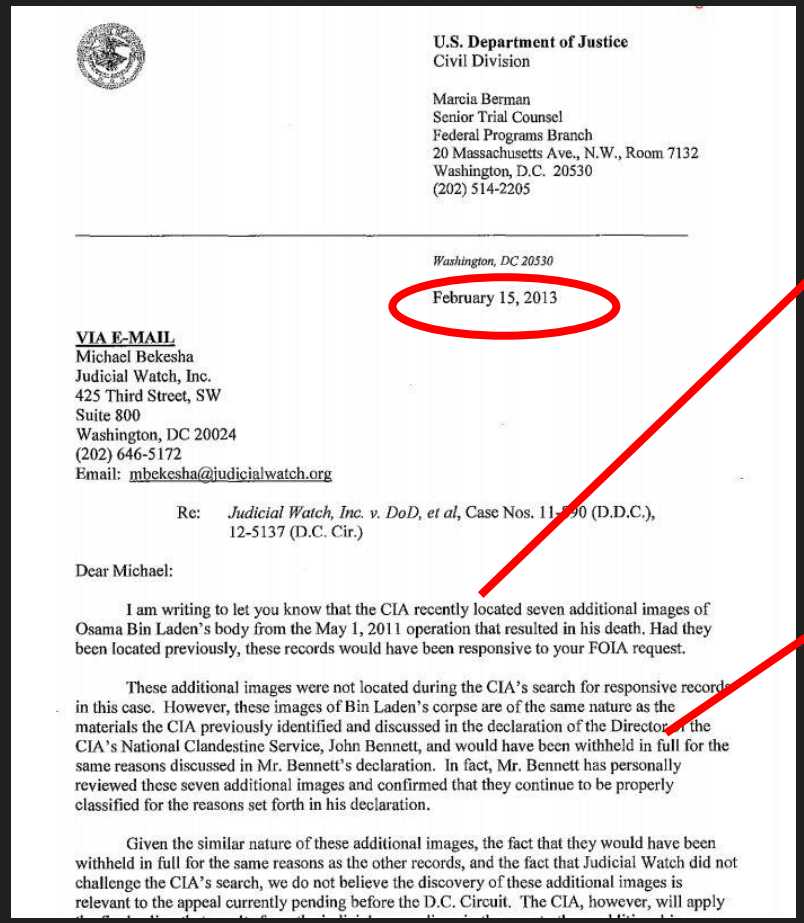
Appeals from United States District Court
for the Eastern District of Missouri - St. Louis

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.

# Even the CIA Makes Mistakes



U.S. Department of Justice
Civil Division

Marcia Berman
Senior Trial Counsel
Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7132
Washington, D.C. 20530
(202) 514-2205

*Washington, DC 20530*

February 15, 2013

**VIA E-MAIL**
Michael Bekesha
Judicial Watch, Inc.
425 Third Street, SW
Suite 800
Washington, DC 20024
(202) 646-5172
Email: mbekesha@judicialwatch.org

Re: *Judicial Watch, Inc. v. DoD, et al*, Case Nos. 11-590 (D.D.C.), 12-5137 (D.C. Cir.)

Dear Michael:

I am writing to let you know that the CIA recently located seven additional images of Osama Bin Laden's body from the May 1, 2011 operation that resulted in his death. Had they been located previously, these records would have been responsive to your FOIA request.

These additional images were not located during the CIA's search for responsive records in this case. However, these images of Bin Laden's corpse are of the same nature as the materials the CIA previously identified and discussed in the declaration of the Director of the CIA's National Clandestine Service, John Bennett, and would have been withheld in full for the same reasons discussed in Mr. Bennett's declaration. In fact, Mr. Bennett has personally reviewed these seven additional images and confirmed that they continue to be properly classified for the reasons set forth in his declaration.

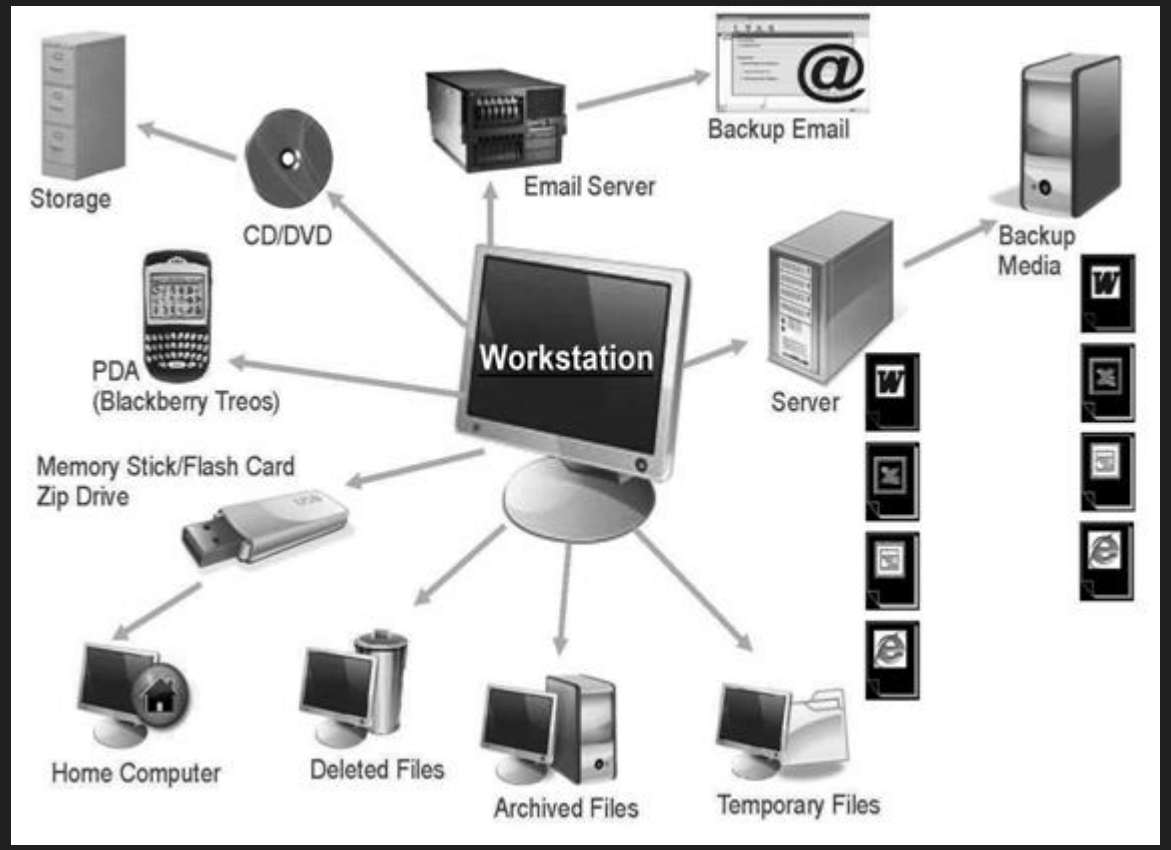
Given the similar nature of these additional images, the fact that they would have been withheld in full for the same reasons as the other records, and the fact that Judicial Watch did not challenge the CIA's search, we do not believe the discovery of these additional images is relevant to the appeal currently pending before the D.C. Circuit. The CIA, however, will apply

*…let you know that the CIA recently located 7 additional images of OBL's body… Had they been located previously, these records would have been responsive to your FOIA request…*

*…we do not believe the discovery of these additional images is relevant to the appeal pending currently before the D.C. Circuit.*

# ESI & e-Discovery

McDonald Hopkins




## *Data Map*

- BEFORE litigation or e-discovery, companies should have a chart where they store data
- This is an IT **and** LEGAL department issue
- *DO YOU HAVE ONE?*

McDonald Hopkins

# *Preservation Demand Letter*

- DO YOU HAVE A CLAIM AGAINST SOMEONE ELSE?
- Notice to (potential) opposing party to preserve necessary evidence and information.
- Typically tells the other side to stop any sort of auto-delete per the company's deletion policy (e.g., think GDPR compliance).
- Could be a setup for spoliation claim.

# *Litigation (or Legal) Hold*

- **WHAT IF YOU GET A PRESERVATION LETER?**
- Notification sent by a company's legal team (typically) to employees and other departments with instructions not to delete or destroy documents
- BEFORE there is a case
- Can be in response to a Preservation Demand or on its own
- This is an INTERNAL process

ESI & e-Discovery

McDonald Hopkins

# *Example: Warrant in Las Vegas Shooter Case*

Learn from law enforcement how to phrase e-discovery requests

**ATTACHMENT "A1"**

**ONLINE ACCOUNT TO BE SEARCHED**

1. This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Accounts") from their inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

# *Warrant in Las Vegas Shooter Case*

***ESI***

which the Government sought from Microsoft (email account provider)

a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;

d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.

e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

# *Warrant in Las Vegas Shooter Case*

**Metadata** which the Government sought from Microsoft (email account provider)

a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;

d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.

e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

# Protect Your Company From Liability

McDonald Hopkins

- WEBSITE: Is your company over-promising?
- PRIVACY POLICY / TERMS & CONDITIONS: Are you over-promising your security measures?
- Did you just copy your Privacy Policies and T&C from somewhere?  Or leave up to website designer?
- TRAINING on risks, especially those targeting your specific industry.
- Have up-to-date policies.  Train.
- Consider encryption.  Deletion policies. GDPR compliance.



# We're Done…

# Two Handouts

# 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

# Nine Ways That Companies Are Getting Hacked

McDonald Hopkins

## Technology Corner

### Nine Ways That Companies Are Getting Hacked

*by Christopher B. Hopkins*

The conventional wisdom regarding data breach and identity theft is that it is not if you will be hacked but *when*. Recent breaches such as Ashley Madison, OPM, Michaels, and Target have led to over 100 million people with potentially compromised credit card and personal information. How is this happening?

Many law firms are jumping on the cyber security bandwagon as they proclaim experience assisting with data breach management. But few lawyers understand how these hacks are being accomplished. Even if you and your client rely on competent IT professionals (as you should), it is important to possess a survey knowledge of how hacks and data breaches occur. This article provides a brief introduction to intrusion and disruption techniques.

**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.

**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.

**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 language called SQL (pronounced "sequel" or alternatively S-Q-L). By re-sending the special character and then a string of code, hackers can learn which databases exist behind the website. After that, they can again send the special character as well as an SQL command to "list tables." From there, a script can be set up to extract data from all revealed databases. Frighteningly, this can all be accomplished from the username and password screen. Recent examples reportedly include 7-11, Sony, and Johns 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.

**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.

**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

# Christopher Hopkins

McDonald Hopkins LLC –
West Palm Beach

This PPT and other posts are available at
www.InternetLawCommentary.com

chopkins@mcdonaldhopkins.com

@cbhopkins

Linkedin.com/in/cbhopkins