Data Breach &
Cyber Security Law

McDonald Hopkins LLC
Attorneys at Law

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, & start up companies.

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 is a DATA BREACH?

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

What are Hackers Trying to Steal?

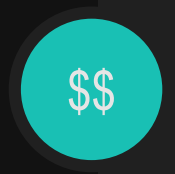
Personally Identifiable Information PII

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 $$$)

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.

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

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

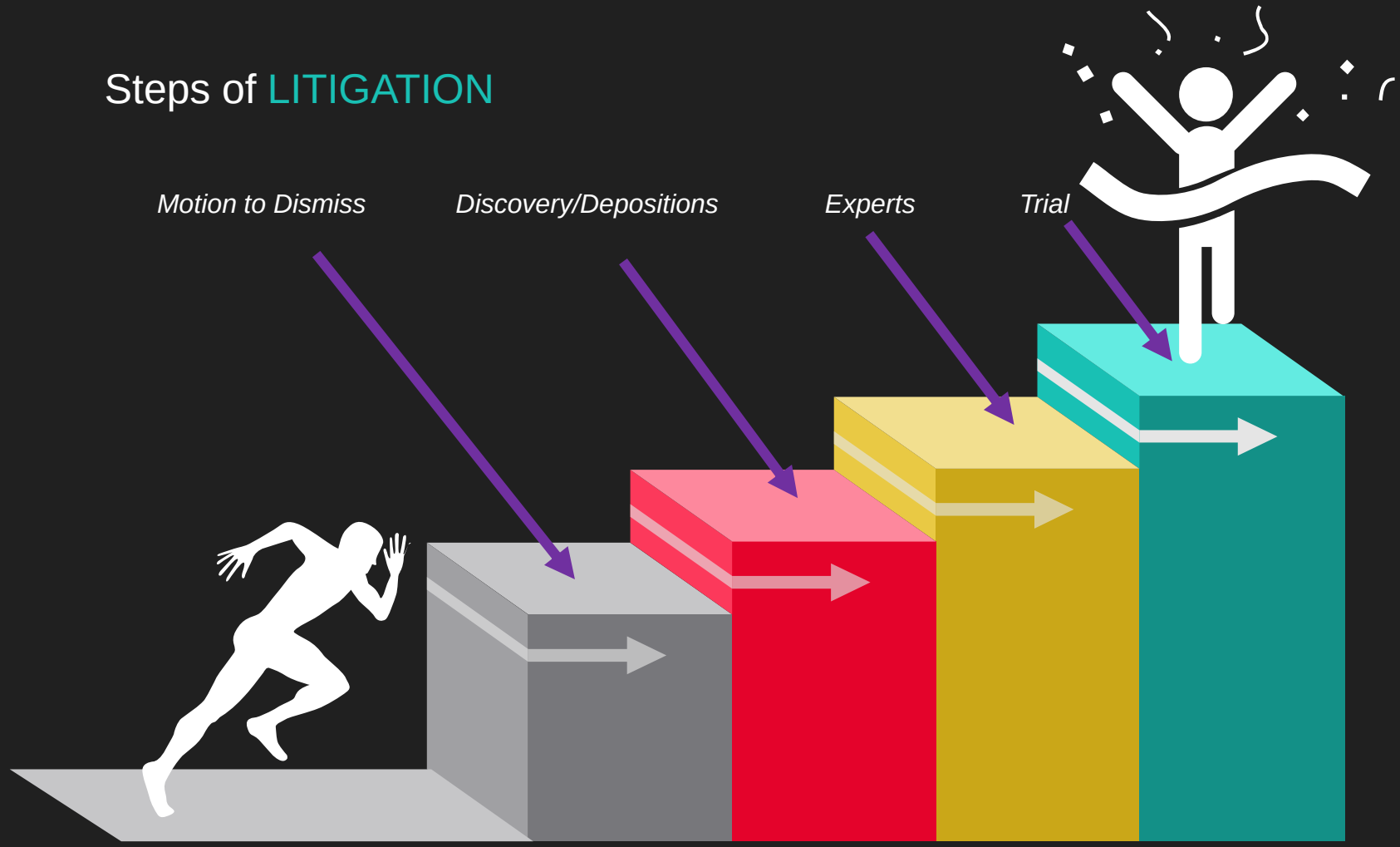
DAMAGES

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

PROVING & WINNING A CASE (any case)

McDonald Hopkins

Steps of LITIGATION



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.

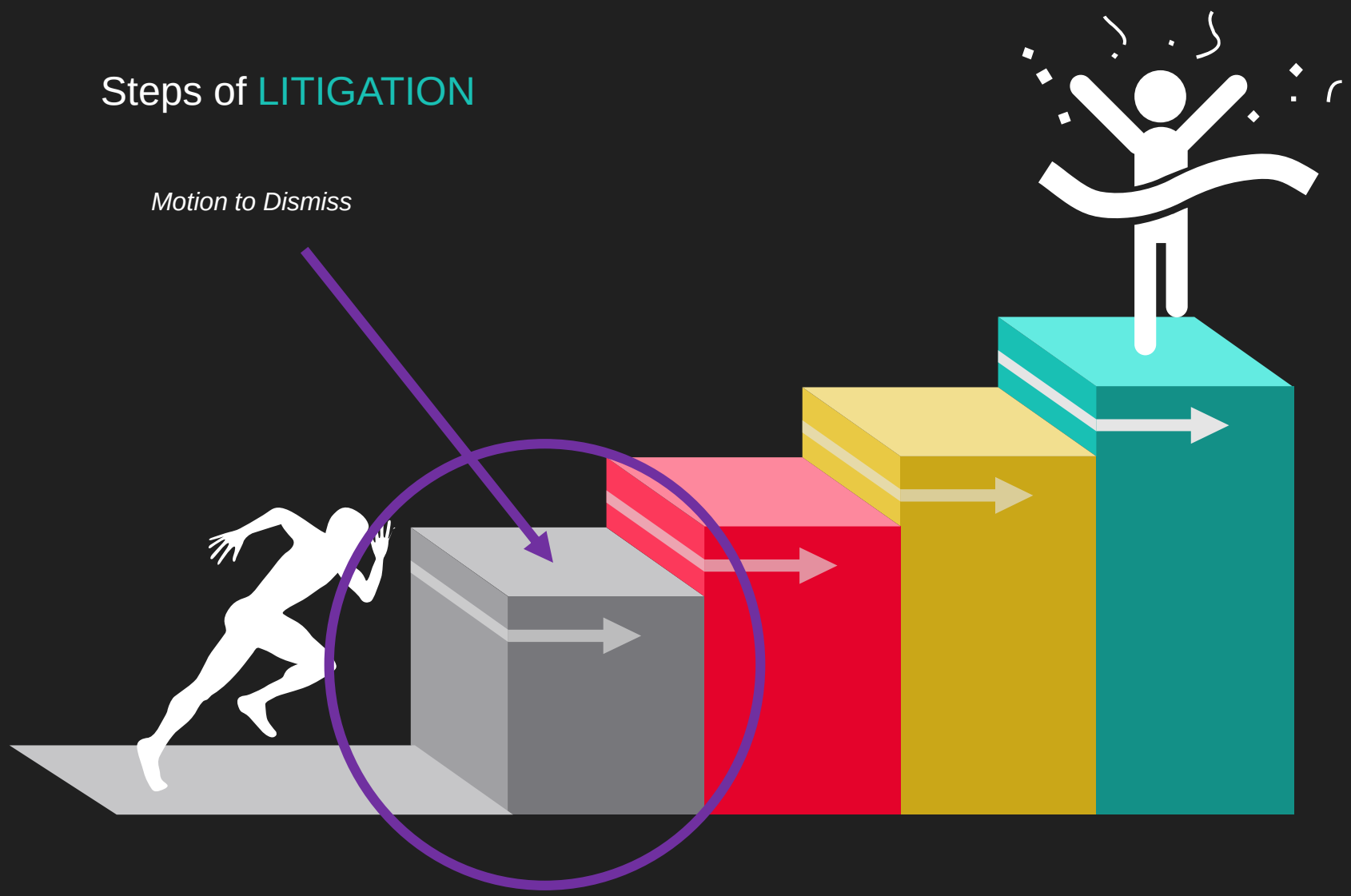
First You Have to Have Standing

PROVING & WINNING A CASE (any case)

McDonald Hopkins

Steps of LITIGATION

Motion to Dismiss



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.

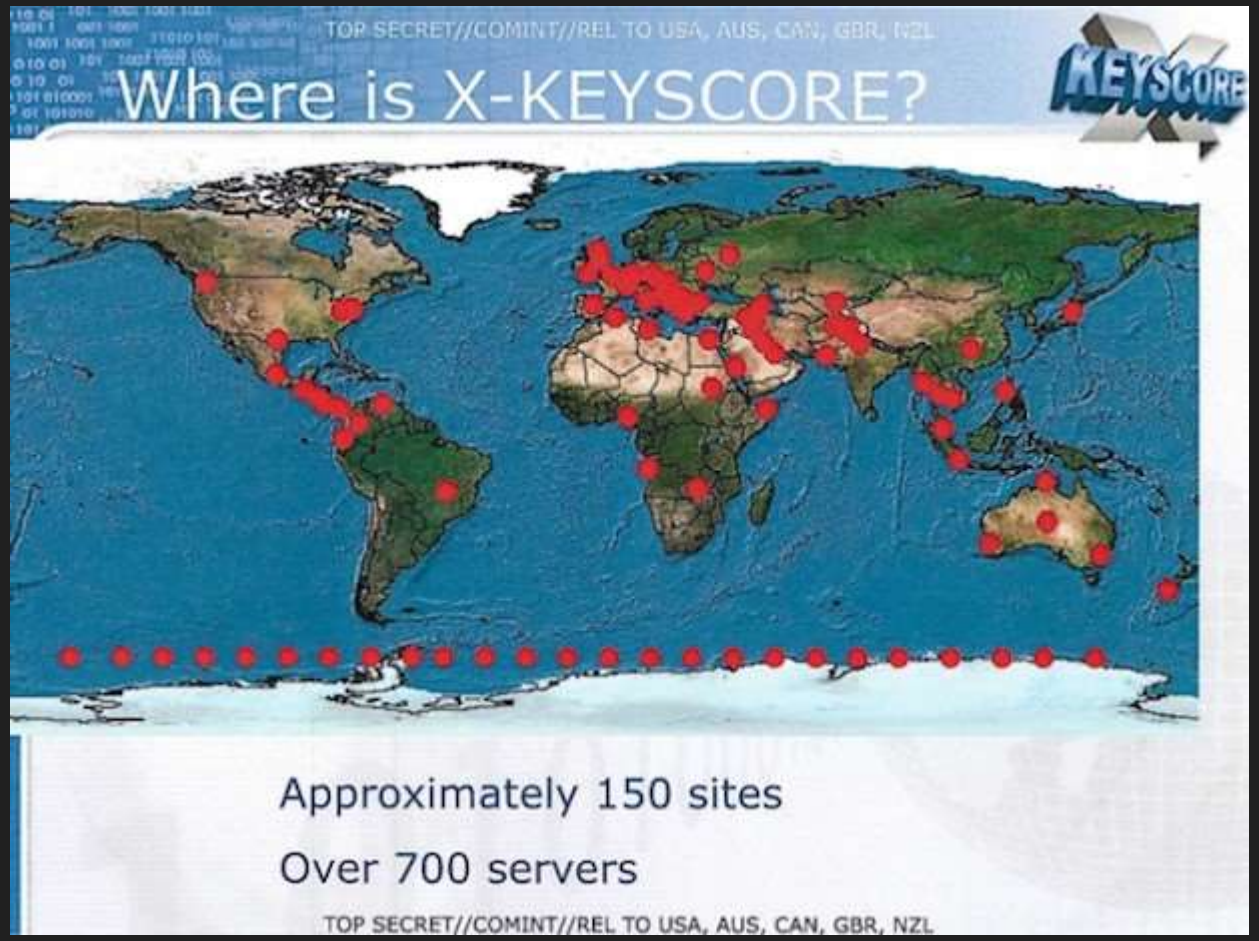
1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

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

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

McDonald Hopkins

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

On the day when the FISA Amendments Act was enacted, respondents filed this action seeking (1) a declaration that §1881a, on its face, violates the Fourth Amendment,

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

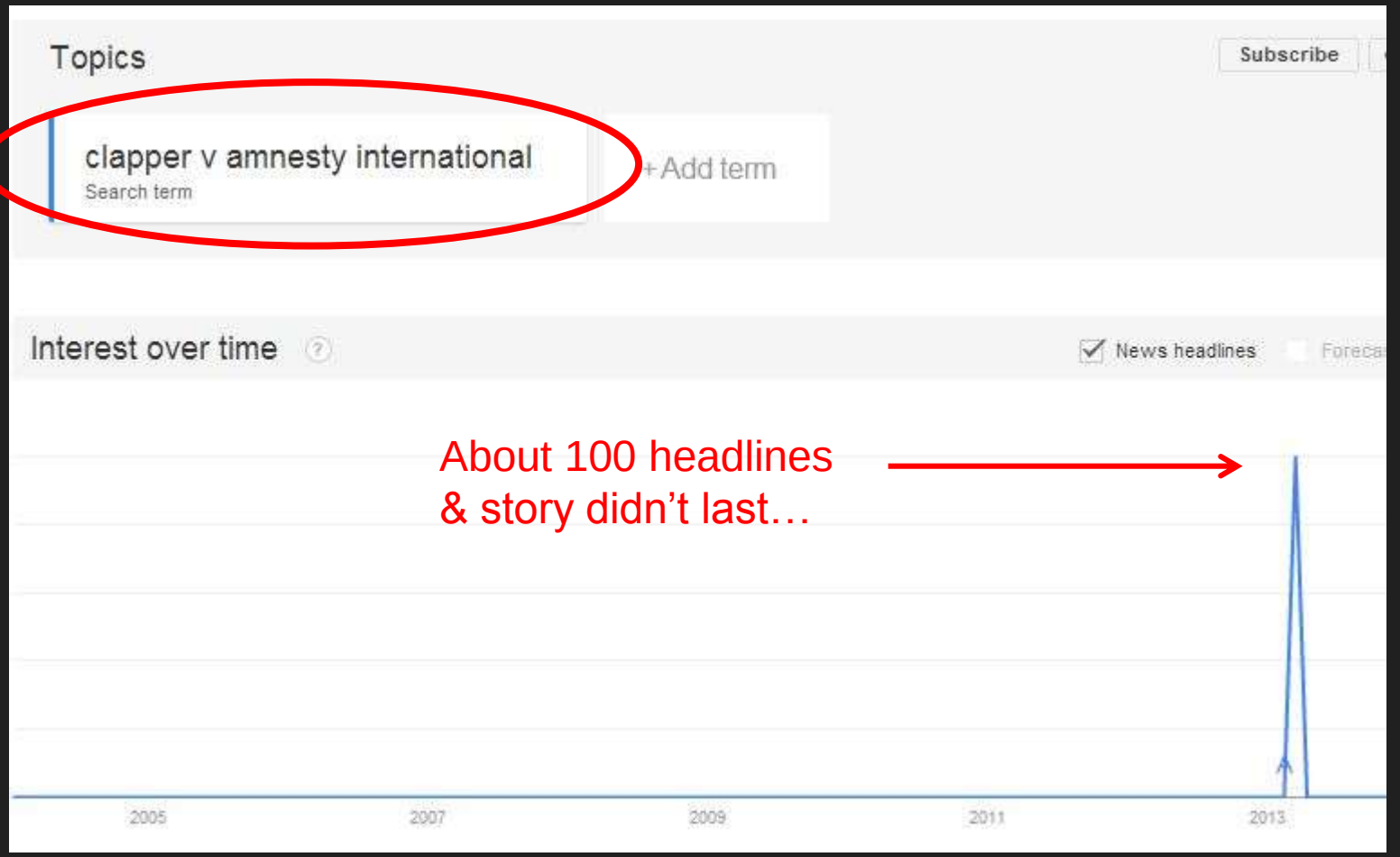
FISA Amendments allow the AG and DNI to surveil non-US persons reasonably believed to be outside the US (normally) after FISC approval.

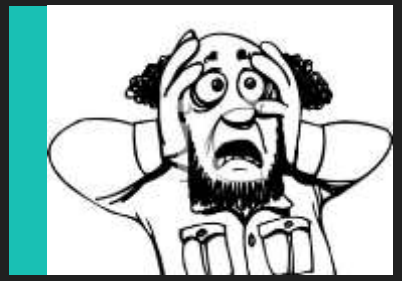
DOESN'T SOUND SO SPECULATIVE NOW…:

1. "Highly speculative" that government will target the parties' communications
2. Petitions 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

Three Months Before The Snowden Revelations

McDonald Hopkins





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.

First You Have to Have Standing

Three Months Before The Snowden Revelations

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.

ELEMENTS OF

Negligence

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

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

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

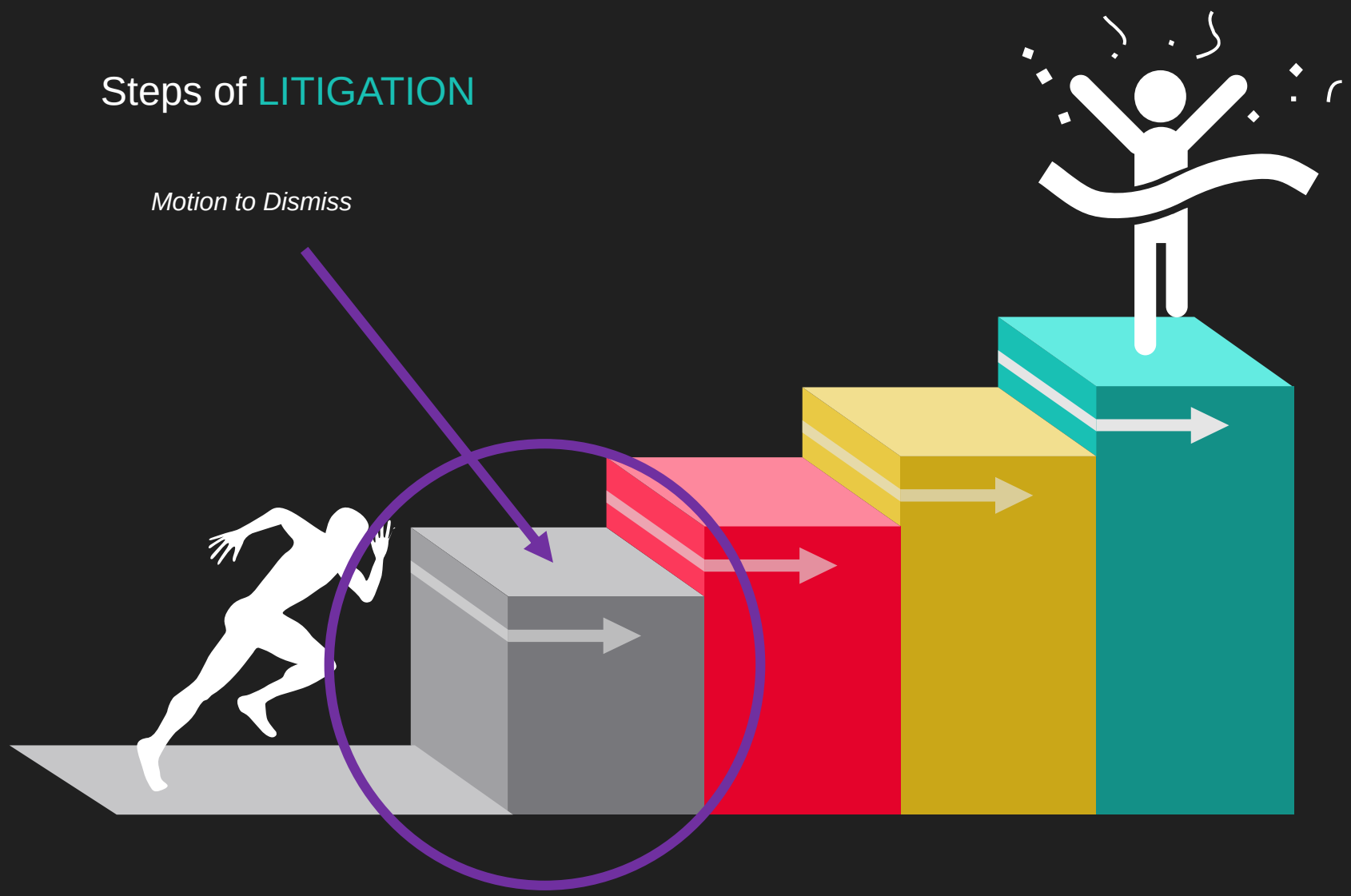
As a result of the defendant's breach, the plaintiff suffered monetary loss.

PROVING & WINNING A CASE (any case)

McDonald Hopkins

Steps of LITIGATION

Motion to Dismiss



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

McDonald Hopkins

"Snowden Lesson"

Plaintiff needs to have Article III Standing

– ability to claim an actual or impending damage –

Before Filing a Lawsuit.

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

McDonald Hopkins

Pro Tip: – Don't Confuse Government Action (NSA) and Suits Between Private Citizens.

The point is that Amnesty International filed suit too soon.

No one care when this case was decided.

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

4 Data Breach Cases

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.

REMIJAS v. NEIMAN MARCUS

Seventh Circuit – July 20, 2015

COURT:

These Allegations are "Dubious":

1. Loss of buying from Neimans (would not have shopped there if they had known of the store's careless approach to security)
2. Lost control of personal information – no authority for a "property right" in credit card numbers. And no PII taken in this case.

The Court Did Not Have to Reach These Issues:

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

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

DISMISSED

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.

IN RE: SuperVALU, INC. Customer Data Security Breach Litigation

Minnesota – January 7, 2016

ALLEGATIONS:

SuerVALU discloses a data breach at over 1,000 stores. Names, payment account numbers, expiration dates, and PINs accessed.

One lead plaintiff alleged that he had fraudulent charge on his credit card. He did not state whether it went through or if he suffered a loss.

Actual Injuries (alleged):

1. Spent time determining whether cards compromised and monitoring their account.
2. Diminished value of PII
3. Invasion of Privacy of PII
4. Lost benefit of the bargain (would not have shopped there)

Impending Injuries (alleged):

1. Increased risk of future losses

IN RE: SuperVALU, INC. Customer Data Security Breach Litigation

Minnesota – January 7, 2016

COURT:

Actual Injuries:

1. Mitigation Costs – "In data breach cases, courts consistently hold that the cost to mitigate against future harm does not constitute an injury in fact unless the future harm being mitigated against itself is imminent."
2. Diminished value of PII – plaintiffs not explain how. If there is such value.
3. Invasion of Privacy of PII – plaintiffs not show concrete injury.
4. Lost benefit of the Bargain – "consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach."

IN RE: SuperVALU, INC. Customer Data Security Breach Litigation

Minnesota – January 7, 2016

Impending Damages:

"In data security breach cases where plaintiffs' data has not been misused following the breach, the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III standing."

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.

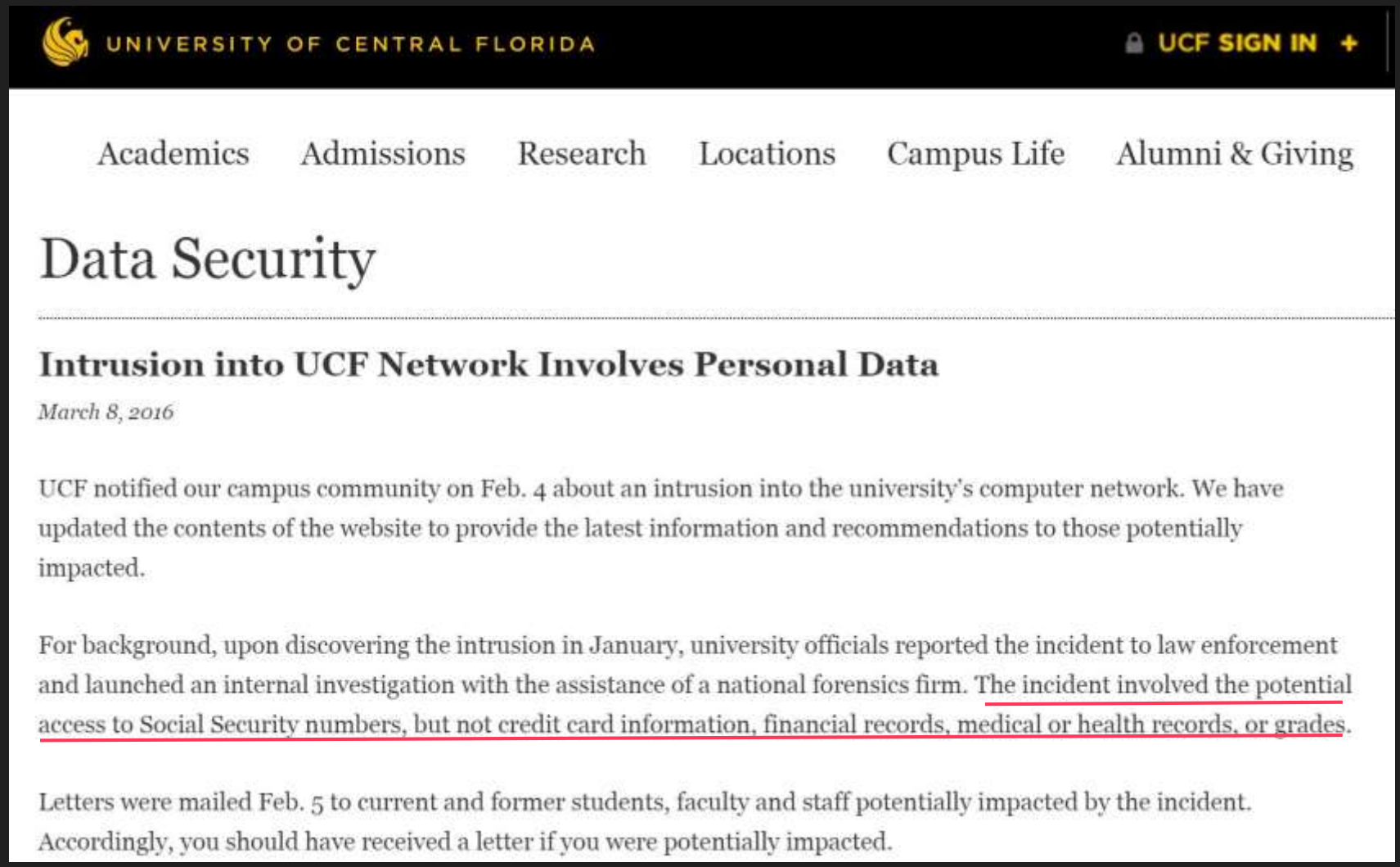
Is There Standing?

University of Central Florida

Data Breach

Standing: UCF Data Breach

McDonald Hopkins



UNIVERSITY OF CENTRAL FLORIDA

UCF SIGN IN +

Academics Admissions Research Locations Campus Life Alumni & Giving

Data Security

Intrusion into UCF Network Involves Personal Data

March 8, 2016

UCF notified our campus community on Feb. 4 about an intrusion into the university's computer network. We have updated the contents of the website to provide the latest information and recommendations to those potentially impacted.

For background, upon discovering the intrusion in January, university officials reported the incident to law enforcement and launched an internal investigation with the assistance of a national forensics firm. The incident involved the potential access to Social Security numbers, but not credit card information, financial records, medical or health records, or grades.

Letters were mailed Feb. 5 to current and former students, faculty and staff potentially impacted by the incident. Accordingly, you should have received a letter if you were potentially impacted.

Furbush & Berkowitz v. UCF

M.D. Fla. – February 5, 2016

ALLEGATIONS:

Hackers accessed names, social, student number, and "other sensitive student information" for 63,000 current and former students.

Actual Injuries (alleged):

1. Lost monetary value of their PII
2. Cost associated with protecting their PII
3. Value of time spent dealing with the breach
4. Loss of right to privacy
5. Other damages

Furbush & Berkowitz v. UCF

M.D. Fla. – February 5, 2016

ALLEGATIONS:

Hackers accessed names, social, student number, and "other sensitive student information" for 63,000 current and former students.

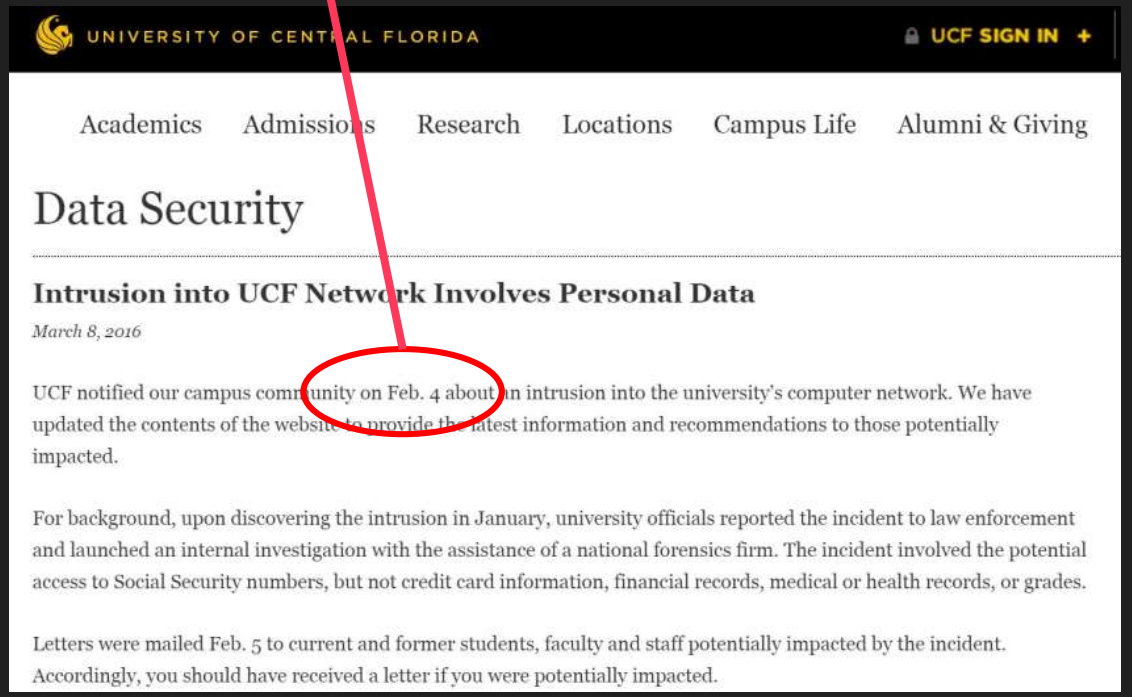
One lead plaintiff alleged that he had fraudulent charge on his credit card. He did not state whether it went through or if he suffered a loss.

Actual Injuries (alleged):

1. Lost monetary value of their PII – *None of the three cases we discussed found "value" in credit card info. Student # may be akin to credit card info. No harm of any kind was alleged, though*
2. Cost associated with protecting their PII – *All three suggest that when "impending" threat is speculative, you cannot manufacture damages. Unlike Reijas, there are not 9,200 instances of fraud.*
3. Value of time spent dealing with the breach – *Same*
4. Loss of right to privacy – *No damages alleged*
5. Other damages – *Too conclusory*

Furbush & Berkowitz v. UCF

M.D. Fla. – February 5, 2016


UNIVERSITY OF CENTRAL FLORIDA

UCF SIGN IN +

Academics Admissions Research Locations Campus Life Alumni & Giving

Data Security

Intrusion into UCF Network Involves Personal Data

March 8, 2016

UCF notified our campus community on Feb. 4 about an intrusion into the university's computer network. We have updated the contents of the website to provide the latest information and recommendations to those potentially impacted.

For background, upon discovering the intrusion in January, university officials reported the incident to law enforcement and launched an internal investigation with the assistance of a national forensics firm. The incident involved the potential access to Social Security numbers, but not credit card information, financial records, medical or health records, or grades.

Letters were mailed Feb. 5 to current and former students, faculty and staff potentially impacted by the incident. Accordingly, you should have received a letter if you were potentially impacted.

Like Clapper, these Plaintiffs wanted to be first…

Hughley v. UCF

Orange County Circuit Court – February 25, 2016

ALLEGATIONS (from press release):

“Former student / basketball team manager claims his bank account was drained not long after the data breach occurred.”

What Will Happen to Standing in Future Data Breach Cases

PREDICTING MORE DATA BREACHES

McDonald Hopkins

01

gemalto
security to be free

Breach Level Index Report

1,673 data breaches resulting in 707 million data records compromised in 2015 alone.

02

U.S. Govt

Federal government is spending **35% more resources** on cyber attacks in 2016. Feb 9, 2016.

03

truShield

Cyber Threat Intelligence Report

We will see **15-40% more ransomware and phishing** attacks in 2016.

04

Inc.

Cybersecurity Predictions

1. **More destructive attacks**
2. Better social engineering
3. Apps will be targeted
4. **IoT hacks increase**
5. More infrastructure security

May Be Harder to Prove Standing With So Many Data Breach Cases

Standing in Data Breach Litigation

McDonald Hopkins

REMIJAS v. NEIMAN MARCUS

> The fact that Target or some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are "fairly traceable" to the data breach at Neiman Marcus. See *In re Target Corp. Data Sec. Breach Litig.*, MDL No. 14–2522 (PAM/JJK), 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014)

> summary judgment on the issue."). If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then "the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." *Price Waterhouse v. Hopkins*, 490 U.S. 228,

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

The Key Case Involves Jumping the Gun

Trying to be the first to file suit can lead a plaintiff to not have sufficient grounds to sue. Ironically, *Clapper* plaintiffs lost only three months before there was profound evidence that everyone may have standing. It became a "nothing" case until data breach cases arose. And, probably contrary to their intent, that case sets the precedent for data breach cases to be dismissed.

3

Data Breach Litigation is Here To Stay

Data breaches are on the rise. Plaintiffs will be able to shift the (costly) burden to large companies to prove that they were not the cause.

Christopher Hopkins

McDonald Hopkins LLC – West Palm Beach

Handouts, Cases & this PPT are at
www.Hopkins.law

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