

A stylized illustration of a lantern on a pedestal. The lantern is green with a yellow flame inside. It sits on a white, conical pedestal. The background is a solid green color.

2019 Boston

ANNUAL CONFERENCE
& SHOWPLACE

Cyber Liability Insurance

By Greg Blake, CIO

Idaho Housing and Finance



 CNN

Hundreds of millions of Facebook records exposed on Amazon cloud servers

New York (CNN Business) A vast collection of data on Facebook users was exposed to the public until recently on Amazon's cloud computing ...


Apr 3, 2019

 Atlanta Journal Constitution

Data breach exposes up to 1.3M Georgia Tech faculty, students

It sounds a bit ironic: a data breach potentially affecting 1.3 million current and former students, faculty and staff members at Georgia Tech, the ...

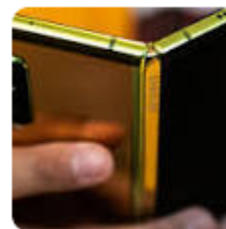
Apr 2, 2019


 Bloomberg Law

No Consolidation for First American Financial Data Breach Suits

No Consolidation for First American Financial Data Breach Suits ... Plaintiffs alleged First American failed to protect the confidential information ...

1 week ago




 Krebs on Security

Breach at Hy-Vee Supermarket Chain Tied to Sale of 5M+ Stolen Credit, Debit Cards

Hy-Vee, based in Des Moines, announced on Aug. 14 it was investigating a data breach involving payment processing systems that handle ...

1 month ago

 Sacramento Bee

Kaiser says data breach exposed information on nearly 1,000 Sacramento-area patients

Kaiser Permanente said Thursday that a data breach had left ... That breach affected 12 million people at Quest Diagnostics, and other ...

1 week ago

 Lexology

Update from LitLand: Reflections on Standing in the OPM Data Breach Litigation: Clapper, Iqbal, and Espionage

The District Court had dismissed the case, saying that plaintiffs – victims of the massive Office of Personnel Management (OPM) data breach ...

1 week ago


In most states failure to report a crime isn't illegal

Then why is a hack different?


Why do you have to report a hack?

Why do you have to report a hack?

Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by **law** is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars (\$2,000), or by imprisonment in the county jail for a period of not ...

 <https://legislature.idaho.gov> › idstat › title28 › sect28-51-105

Section 28-51-105 – Idaho State Legislature

 <https://law.justia.com> › subtitle-7 › chapter-110 › section-4-110-105 ▾

§ 4-110-105. Disclosure of security breaches :: 2016 Arkansas ...

(a) (1) Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of **Arkansas** whose unencrypted personal information ...

 <https://www.revisor.mn.gov> › statutes › cite › 325E ▾

Sec. 325E.61 MN Statutes - Revisor of Statutes

(a) Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted ...

You **HAVE** to report a hack.

Once you do, bad things
happen to **YOU**.

What you will get sued for

Data Breach Reporting Violation

Negligence

Breach of contract

Shareholder suit

Regulatory/statutory violation

HIPAA; GLB; COPPA

GDPR, CCPA (California), Massachusetts,
Illinois (biometric data)

Standing or Summary Judgment



Beginning
of Case

Discovery

Motion



Standing
or
Summary
Judgment



Article III
Standing?

- Injury
- Causation
- Redressability



Trial



Dismissed

What is Standing

Article III

Three constitutional standing requirements

- You must have suffered or will suffer an injury soon
- The injury was caused by the defendant's conduct
- And a favorable federal court decision is likely to redress the injury



Standing

Data Breach Lawsuit Survives Motion to Dismiss

April 28, 2017

Updates

In an April 13, 2017 decision in *Walters v. **Kimpton Hotel***,¹ a California federal judge rejected the bid of hotel chain Kimpton Hotel and Restaurant Group, LLC to dismiss a proposed class action arising from a data breach last year. Judge Vince Chhabria found that the named plaintiff sufficiently alleged imminent harm to establish standing notwithstanding the absence of allegations that his **personal information** had been misused.

“However, Judge Chhabria allowed implied contract, negligence and California unfair business practices claims to continue.”

Ninth Circuit Finds Data Breach Customers Have Initial Standing to Sue

APRIL 2018 COMMENTARIES

In Short

The Situation: Relating to a 2012 data breach lawsuit against **Zappos.com**, a district court had found that a certain group of plaintiffs lacked standing to sue because they "failed to allege instances of actual identity theft or fraud."

The Development: In reversal of the lower court's decision, a unanimous Ninth Circuit panel has resurrected claims against Zappos.com, finding that the "imminent" risk of identity theft from the breach was enough to establish **standing** to sue.

Looking Ahead: Ninth Circuit litigants should consider the decision in determining how to respond to a data breach complaint.

Fourth Circuit Decision Seizes Middle Ground on the Issue of Standing in Data Breach Cases

Wednesday, June 20, 2018

In the latest decision in the concerning standing in data breach cases, the Fourth Circuit has vacated a district court's dismissal and reinstated putative class action data breach litigation against the **National Board of Examiners in Optometry Inc.,** ("NBEO"). In *Hutton v. National Board of Examiners in Optometry, Inc.*, the court ruled that the plaintiffs alleged sufficient injury to meet the Article III standing requirement by virtue of hackers' theft and misuse of plaintiffs personally identifiable information ("PII"), notwithstanding the absence of any allegation that the misuse had resulted in pecuniary loss to the plaintiffs. In so ruling, the Fourth Circuit struck a middle course on the question of when misuse of sensitive PII results in a sufficient injury to confer standing to sue in federal court.

In re: U.S. Office of Personnel Management Data Security Breach Litigation

Court: US Court of Appeals for the District of Columbia Circuit

Docket: 17-5117

Opinion Date: June 21, 2019

These consolidated appeals stemmed from the cyberattack of multiple **OPM** databases that resulted in the data breach of sensitive personal information from more than 21 million people. Plaintiffs alleged that OPM's cybersecurity practices were inadequate, enabling the hackers to gain access to the agency's database of employee information, in turn exposing plaintiffs to heightened risks of identity theft and other injuries. The district court dismissed the complaints based on lack of Article III standing and failure to state a claim. The DC Circuit held that both sets of plaintiffs have alleged facts sufficient to satisfy Article III standing requirements; the Arnold Plaintiffs have stated a claim for damages under the Privacy Act, and have unlocked OPM's waiver of sovereign immunity, by alleging OPM's knowing refusal to establish appropriate information security safeguards.

A Closer Look At Barnes & Noble Data Breach Ruling

By Joshua Jessen and Ashley Van Zelst (May 7, 2018, 1:12 PM EDT)

Last month, a three-judge panel of the Seventh Circuit issued an opinion in *Dieffenbach v. Barnes & Noble Inc.*[1] — a proposed data breach class action — that appeared to suggest that a plaintiff who has adequately pled an injury-in-fact for purposes of Article III standing has per se pled damages sufficient to withstand a motion to dismiss for failure to state a claim upon which relief may be granted under Federal Rule of Civil Procedure 12(b)(6). A closer inspection of the opinion, however, reveals that the holding was not so broad, and that there will continue to be circumstances in data breach cases where a plaintiff's complaint may be able to survive an Article III standing challenge but will still be dismissed for failure to state a claim due to the absence of cognizable damages. One of those circumstances is the increasingly common situation where a plaintiff has alleged a future risk of identity theft but has not yet suffered any actual harm.

No Celebration For **Yahoo!**: Data Breach Claims Survive Motion to Dismiss

April 12, 2018 by Carlton Fields

Defendants again moved to dismiss, and, last month, the court granted the motion in part. As with most data breach class actions, this one raised the issue of standing — specifically, for purposes of the UCL. In particular, with regard to claims under the unfair and unlawful prongs, defendants argued plaintiffs did not establish that they had “lost money or property,” as required for UCL standing. The court partially agreed, dismissing the UCL claims of certain plaintiffs who alleged only that they were at risk for — as opposed to had suffered — identity theft, holding that the threat of future harm did not suffice to establish **standing**. However, the court refused to dismiss the claims of the plaintiff representing paid users, who alleged he expected to receive secure email services and would not have paid for his account in the absence of such assurances. Relying on the California Supreme Court’s decision in *Kwikset Corp. v. Superior Court* and the holding of the Northern District of California in *In re Anthem, Inc. Data Breach Litigation*, the court found these benefit of the bargain losses established **standing** for purposes of the UCL.

Take-Aways from the cases

1. Standing
2. Cases will increase, not decrease
3. Plaintiffs lawyers will be emboldened
4. Importance of attorneys' fees awards
5. How much is this going to cost?
6. Are you insured?

Get Good Cyber Liability Insurance

Cyber Liability Insurance should cover:

- Data Breach Reporting Obligations
- Online advertising injury
- Restoring personal identities of affected customers
- Recovering compromised data
- Repairing damaged computer systems
- Related privacy lawsuits against you
- Theft of IP

Encrypt Your Data

28-51-104. DEFINITIONS. For purposes of sections 28-51-104 through 28-51-107, Idaho Code:

...

(2) "Breach of the security of the system" means the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information

THANK YOU!

- Greg Blake, CIO, gregb@ihfa.org
- Additional Credit: Brad Frazer Attorney, Brad Frazer, Brad.Frazer@hawleytroxell.com

Typical premiums for cyber insurance

Size of Company (Based on Revenue)	Small Companies (Less than \$100 Million)	Midsized Companies (\$100 Million - \$1 Billion)	Large Companies (More than \$1 Billion)
Coverage	\$1 – 5 million	\$5 – 20 million	\$15 – 25+ million
Yearly Premium (Cost for Coverage)	\$7,000 – \$15,000 per million in coverage	\$10,000 - \$30,000 per million in coverage	\$20,000 - \$50,000 per million in coverage

Typical Coverage Sublimits (Restrictions on Payout)

Sub-limits can restrict payouts on a single aspect of coverage from 10 – 50% of the total coverage

Notification Cost	\$100,000 - \$500,000 limit	\$500,000 - \$2 million limit	\$1.5 - \$2.5 million limit
Crisis Management Cost	\$250,000 - \$1.25 million limit	\$1.25 - \$5 million limit	\$3.75 - \$6.25 million limit
Legal and Regulatory Defense Expense	\$500,000 - \$2.5 million limit	\$2.5 million - \$10 million limit	\$7.5 - \$12.5+ million limit

Source: Deloitte research on insurance provider Web sites