TABLE OF CONTENTS

ARTICLES >>

Data Breach Basics..................................................................................................................2
By Daniel B. Heidtke
An overview of data breach issues and litigation.

Cryptocurrency Claims and Insurance Issues.................................................................5
By Dominic Spinelli
A discussion of recent cryptocurrency claims and their impact on the insurance industry.

NEWS AND ANNOUNCEMENTS >>

ABA Midyear Meeting...........................................................................................................7
February 1-4, 2018

Publish Your Article with YLD TIPS..................................................................................8
If you an idea for an Article or 101 Practice Series Article, contact Dominic Spinelli at
dspinelli@peabodyarnold.com.
**ARTICLES**

**Data Breach Basics**  
By Daniel B. Heidtke

$100,000 in hush money.\(^1\) That was the news in November 2017 when the ride-hailing service, Uber, disclosed it had been the victim of hacking.\(^2\) Well, in reality, about 57 million riders and drivers that use Uber’s service were victims and Uber failed to disclose the hack (or the payment to the hackers) for almost one year.\(^3\)

Uber was not the first and, unfortunately, will not be the last company that will be the target of identity thieves. The problem is an indefinite, expensive reality. In fact, one recent study estimated that “cybercrime damages” will cost $6 trillion *annually* by 2021.\(^4\)

*What’s a ‘breach’?* The Identity Theft Resource Center (ITRC), a non-profit organization created to provide assistance and education concerning data privacy and breaches, defines a “breach” as “an incident in which an individual name plus a Social Security number, driver’s license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure. This exposure can occur either electronically or in paper format.”\(^5\) The ITRC has identified five “breach categories,” including business, educational, medical/healthcare, government/military, and banking/credit/financial. According to the ITRC, in 2015 the greatest frequency of breaches were in the “business”\(^6\) category, which at that time averaged nearly one breach per day.\(^7\) The largest number of records exposed by breaches were in the “medical/healthcare” category – a total of 121,629,812 records were exposed by approximately 276 breaches in 2015.\(^8\) In sum, this is a frequent, expensive and widespread issue, and the “clean-up” alone can cost millions of dollars.\(^9\)

Before the “clean-up,” however, comes notice. There are a myriad of laws applying to the protection of personal, private information. When the protection of such information breaks down and personal, private information is lost, exposed or stolen, there is another equally complex and interwoven set of federal and state laws requiring notice to those affected by the “breach.” “Expedient” and “without unreasonable delay,” provided in “plain language”—these timing, content and manner requirements are littered throughout statutes explaining what companies (large and small) must do when they learn that personal, private information has

---

2 Id.  
3 Id.  
6 According to ITRC, “This category encompasses retail services, hospitality and tourism, professional, trade, transportation, utilities, payment processors and other entities not included in the other four sectors. It also includes nonprofit organizations, industry associations and nongovernment social service providers as well as life insurance companies and insurance brokers (non-medical).”  
7 There were 312 breaches in 2015 in the “business” category, which were identified by the ITRC as of December 29, 2015. *See* footnote 6, *supra*.  
8 Id.  

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
been compromised. So that you – the reader – may know what to expect (or how to act) when personal, private information has been compromised, a few of the requirements are surveyed and compared below.¹⁰

Under California law, certain businesses operating in California that “own or license computerized data that includes information” are required to give notice to any California resident of a “breach in the security of the data.”¹¹ The notification requires “plain language,” including information under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.”¹² In addition, if the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months.¹³ If more than 500 California residents are notified of the breach, the entity responsible must provide notice to the California Attorney General.

Under Illinois law, “data collectors”¹⁴ that own or license personal information concerning an Illinois resident must notify the resident of a breach following discovery or notification of the breach. Like California, Illinois requires that the disclosure notification is made in the “most expedient time possible and without unreasonable delay,” consistent with any measures necessary “to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.”¹⁵ Unlike California, Illinois does not place a threshold number of affected-residents before requiring notice to the state attorney general. Instead, if the entity is required to provide notice to the Department of Health and Human Services, then it must also provide notice to the Illinois Attorney General’s office within 5 days of providing notice to the Department of Health and Human Services.¹⁶

Under Nevada law (just like California and Illinois), “data collectors”¹⁷ that own or license computerized data which includes personal information shall disclose – in the “most expedient time possible” – any breach to any Nevada resident “whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”¹⁸ Rather than notifying the Nevada Attorney General, however, if the “data collector” is required to notify “more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency” that compiles and maintains files on

---

¹⁰ The statutes discussed herein are only a few of the many laws that may apply to a particular person or entity in a particular state, and do not include all of the laws applicable within the state discussed. For instance, despite discussing the requirements under California Civil Code section 1798.82, this article does not discuss requirements under another California law (California Health & Safety Code section 1280.15), which pertains to the disclosure of personal, private health information by certain regulated entities (e.g., health facilities, home health agencies). Thus, you should not rely upon this article as an exhaustive list of statutes applying to the states discussed herein.


¹⁴ A “data collector,” “may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.” 815 ILCS 530/5.

¹⁵ 815 ILCS 530/10.

¹⁶ 815 ILCS 530/50.

¹⁷ A “data collector,” means “any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.” NRS 603A.030.

¹⁸ NRS 603A.220(1).

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
consumers on a nationwide basis.19 “Consumer reporting agency” in this context means a company that regularly aggregates public records and credit account information “for the purpose of furnishing consumer reports to third parties bearing on a consumer’s credit worthiness, credit standing, or credit capacity.”20 Thus, under Nevada law, an entity that is required to notify more than 1,000 people about a breach must also notify companies like Equifax, Experian and Transunion.

Under Washington law, the requirements are similar to the other states mentioned above, i.e., any “person or business that conducts business” within the state, must provide notice of a breach within a reasonable time after notice or discovery of the breach.21 But, opening the potential for ambiguity, Washington law does not require notice “if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm.”22 Additionally, in Washington, although notice must be provided within a “reasonable time,” notice must be provided to affected consumers and the Washington Attorney General’s office within forty-five days after the breach was discovered.23 In some sense, therefore, Washington has set a definition of what is “reasonable,” i.e., less than forty-five days.

After notice, comes the “clean-up.” The clean-up may come in many forms (e.g., criminal investigations, insurance claims, credit freezes) – one form no company wants, however, is litigation. While state laws may expressly provide a remedy for the company that was targeted by the breach against the person(s) that “unlawfully obtained or benefited from” the breach, the affected-consumers are often left without specific, statutory remedies.24 For instance, while the Stored Communications Act, 18 USC § 2701 et seq., may provide an additional source of liability,25 legal liability arising out data breaches is typically based upon state law for negligence and breach of (implied) contract. For the consumer, however, many defendants (typically the company that was breached), are successful in asserting that in order for a consumer to prevail, the consumer must show his or her data was actually used, i.e., some actual harm (often articulated as failing to satisfy the “standing” requirement). Thus, many consumers may feel aggrieved without the possibility of redress.

Regarding allegations of actual harm, there is a growing split amongst courts concerning whether a plaintiff must be able to demonstrate actual harm in order to bring a statutorily-created cause of action. There was some hope that Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016), which addressed a plaintiff’s standing to bring suit under the Fair Credit Reporting Act would resolve, or at least provide guidance on, the issue.26 For example, in Spokeo, the Supreme Court held that plaintiffs who allege violations of statutes that contain a private right of action and statutory damages must establish both an “invasion of a legally protected interest”

---

19 NRS 603A.220(6).
20 NRS 603A.217(6); 15 U.S.C. § 1681a(p).
21 RCW 19.255.010(1).
22 Id.
23 RCW 19.255.010(16); if the entity is subject to Washington state’s insurance regulations, the entity has two business days to provide notice to the insurance commissioner. WAC 284-04-625(2).
24 See NRS 603A.900.

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
and “concrete and particularized” harm, in order to satisfy Article III’s standing requirement. At least according to a few commentators, the defense bar “cheered” the result in *Spokeo*, believing that the “concrete and particularized” harm requirement would lead to a higher-threshold for plaintiffs and quicker dismissals for defendants. Not necessarily.

In *Spokeo*, the Court recognized that allegations concerning the “risk of real harm” would meet the “concrete and particularized” harm requirement that it enunciated. As the Court explained, “[c]oncrete’ is not, however, necessarily synonymous with ‘tangible.’ Thus, although a “bare procedural violation, divorced from any concrete harm” is insufficient to satisfy the injury-in-fact requirement of Article III of the United States Constitution, “particular procedural violations” may still “entail a degree of risk sufficient to meet the concreteness requirement.” From this, as Bradford C. Mank explains, the *Spokeo* decision failed to “directly address and leaves open the question of whether a data breach without any financial losses constitutes a concrete injury for Article III standing.”

The lesson from all of this? Well, “it depends.” We have learned that data breaches are an expensive and more frequent reality. We have learned that the notice-of-breach requirements are built with a patchwork quilt of state and federal laws, often requiring “expedient” action with “reasonable” explanations. And, we have learned that although some states have specific statutory remedies for the companies that were hacked or had information stolen, consumers (who have had their information lost or stolen) might face a difficult path in their pursuit to hold a company liable. This is a developing area, and, it is fair to assume that statutes and case law will continue to be adopted, amended and abandoned for the foreseeable future – stay tuned.

Danny is a trial attorney with Duane Morris LLP, a law firm with offices spread throughout the United States, London, Singapore, Vietnam, Oman, Myanmar, Shanghai and Taiwan. Danny is based in the Los Angeles and Las Vegas offices of Duane Morris, and is licensed to practice law in California, Illinois, Nevada and Washington. Danny has an active commercial litigation practice, with a particular focus on complex litigation, including insurance coverage, products liability and class actions. He can be reached at dbheidtke@duanemorris.com.

**Cryptocurrency Claims and Insurance Issues**

By Dominic Spinelli

In 2017, cryptocurrencies and in particular bitcoin went mainstream. In its most basic form, cryptocurrency is decentralized digital currency. Oxford Dictionaries define the term as “a digital currency in which encryption techniques are used to regulate the generation of units of currency

---

27 See, e.g., McNicholas and Nye, supra, note 26.
29 *Spokeo*, 136 S. Ct. at 1549.
30 Id.
31 Id., at 1550.

© 2018 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
and verify the transfer of funds, operating independently of a central bank.” While much has been said about the viability of cryptocurrencies as an investment product, this article focuses on insurance issues arising out of digital currency.

In recent months, several claims have emerged related to cryptocurrencies. In particular, there has been a growing trend of securities class action lawsuits arising out of Initial Coin Offerings (“ICOs”). An ICO is a means by which funds are raised for a new cryptocurrency venture. ICOs are similar to initial public offerings (“IPOs”) and crowdfunding. In 2017, there were 235 ICOs, raising over $3.7 billion. See https://www.coinschedule.com/stats.html.

At the same time, ICOs have come under scrutiny by the U.S. Securities and Exchange Commission (“SEC”) and have led to several class action lawsuits, including, to date, at least five lawsuits against ICO sponsors Centra Tech, Monkey Capital, ATBCoin, Tezos, and Giga Watt. The first such lawsuit was filed on October 25, 2017 against Tezos alleging that its $232 million ICO was an unregistered sale of securities under federal law and that many of the representations that the offering’s sponsors made were “either exaggerations or outright lies.” See Baker v. Dynamic Ledger Solutions, Inc., Case No. 17-562144, filed in the Superior Court of the State of California, County of San Francisco. The complaint alleges the unauthorized sale of securities in violation of Section 5 of the Securities Act, fraud in the sale of securities under Section 17 of the Securities Act, false advertising, unfair competition, and alter ego liability. Three subsequent class action lawsuits have been filed against Tezos arising out of its ICO.

On December 13, 2017, a class action lawsuit was filed against Centra Tech alleging that Centra’s $30 million ICO was an unregistered sale of securities under federal law. See Rensel v. Centra Tech, Inc. et al., Case No. 17-cv-24500, filed in the U.S. District Court for the Southern District of Florida. The complaint alleges that Centra “made a feeble attempt to portray the Centra ICO as the sale of utility-based tokens that were not securities, shares or investments.” The complaint asserts violations of Sections 12(a) and 15(a) of the Securities Act of 1933.

On December 20, 2017, a class action was filed against Monkey Capital alleging that it fraudulently promoted an ICO and engaged in an unregistered offering and sale of securities that violated numerous state and federal securities laws, including Sections 5, 12(a), 15, and 17(a) of the Securities Act of 1933. See Hodges, et al. v. Monkey Capital, LLC, et al., Case No. 17-cv-81370, filed in the U.S. District Court for the Southern District of Florida.

On December 21, 2017, a class action was filed against ATBCoin alleging that it intentionally misled investors about the technological capabilities of its cryptocurrency venture, the potential for investment losses, and the nature of the ICO itself. See Balestra, et al. v. ATBCoin LLC, et al., Case No. 17-cv-10001, filed in the U.S. District Court for the Southern District of New York. The complaint alleges violations of the Securities Act of 1933. As an interesting aside, the complaint also alleges that Herbert Hoover, a co-founder of ATBCoin, deceptively claimed that he is a descendent of former U.S. President Herbert Hoover.

Most recently, on January 3, 2018, a class action as filed against Giga Watt alleging that it conducted an unregistered securities offering. See Stormsmedia, LLC, et al. v. Giga Watt, Inc., et al., Case No. 17-cv-00438, filed in the U.S. District Court for the Eastern District of
Washington. The complaint alleges violations of Sections 5(a) and 5(c) of the Securities Act of 1933, and rescission of contract.

The lawsuits noted above remain in the early stages. It is almost certain, however, that 2018 will result in increased targeting of ICOs and new legal theories. Insurers will need to determine the extent to which existing liability coverages will respond to such claims. The exposure for the types of allegations made in the ICO securities class actions would traditionally be covered by directors and officers (“D&O”) insurance. However, there are several potential coverage barriers that will need to be addressed by insurers going forward. First, D&O insurance for private companies generally exclude coverage for claims arising out of public offerings of securities. Second, insurers will need to determine the extent to which such claims that are rooted in restitution or disgorgement of ill-gotten gains are covered loss under D&O insurance. Third, insurers will need to determine the extent to which such claims are excluded from coverage based on exclusions for fraudulent and intentional conduct and for unlawful profits. While these and other issues under existing liability coverages are certain to unfold in 2018, the insurance industry will also need to determine how cryptocurrency-related risks can be underwritten going forward.

Dominic Spinelli is an attorney with Peabody & Arnold in Boston, Massachusetts. Dom represents insurers in matters involving directors and officers, employment practices, professional liability, and general liability insurance coverage.

NEWS AND ANNOUNCEMENTS

ABA Midyear Meeting

We hope to see you at the ABA Midyear Meeting in Vancouver, British Columbia on February 1-4, 2018. Columbia. ABA TIPS will host specific programming for the YLD. Be sure to join us at the following events:

(1) TIPS Public Service Project with Young Lawyers Division – 9:00 AM – 12:00 PM on Friday, February 2, 2018, in the Oceanview Suite 7 (R Level) at the Pan Pacific Vancouver Hotel.

(2) Trial Academy for YLD – Evidence Conga Line – 4:00 PM – 5:00 PM on Friday, February 2, 2018 at Hyatt Regency Vancouver – Balmoral, 3rd Floor.

(3) TIPS Midyear Reception with Young Lawyers Division – 6:00 PM – 7:30 PM on Saturday, February 3, 2018, at Cypress Suite (R Level) at the Pan Pacific Vancouver Hotel.

You can register for Midyear at https://www.americanbar.org/portals/midyear-meeting.html.
Publish Your Article With YLD TIPS!

YLD TIPS is a great opportunity to be a published. If you have an idea for an article and are interested in authoring an article for future newsletters, please contact Dominic Spinelli at dspinelli@peabodyarnold.com.

If not a newsletter article, consider publishing a 101 Practice Series Article with the YLD TIPS Committee. The 101 Practice Series Articles are specifically geared toward the young lawyer. These articles provide other young attorneys practical information and training in both substantive and practical aspects of law practice. 101 Practice Series Articles can include tips, lists, bullet points, examples, good quotes, lively writing, and other techniques to facilitate the readers’ grasp of information. Do not underestimate how your experience can help other young lawyers.

If interested, please contact Dominic Spinelli at dspinelli@peabodyarnold.com.