CU*ANSWERS
A Credit Union Service Organization

What's "New" In Cybersecurity (2017)

Litigation and Enforcement Actions

May 24, 2017

An **CU*Answers** Whitepaper

Contents

Executive Overview

When discussing cybersecurity enforcement and legislation, describing what's "new" can be a challenge. After all, some of the fundamental cybersecurity legislation, such as HIPAA and GLBA are either nearing or have surpassed 20 years in age. The term "cybersecurity" itself replaces old nomenclature such as "information security" or "data security," and is mostly 'old wine in new bottles' – something old presented as a new. What is new in cybersecurity law isn't so much "new" as observable trends regarding regulator activity and the court rulings. In addition, these cases tend to take a very long time to resolve, with advances in technology rapidly outpacing the ability of the law to absorb the changes. Cases can take a very long time to resolve, with new breaches, regulatory actions, and court cases taking over media and public attention.[1]

However, cybersecurity breaches are rapidly becoming both unavoidable and the norm. Every organization worldwide appears to be falling into one of two categories:

- either the organization has been breached (whether the organization knows it or not); or
- the organization *will be* breached (whether the organization is ready or not).

Therefore, the key takeaways from any review of the trends in cybersecurity law should be what steps an organization can do to reduce the potential impact of a cybersecurity breach. The good news is certain trends are becoming clearer, allowing organizations to take steps to understand and protect themselves from the risks of a cybersecurity incident. Four key trends appear to be emerging from the morass of lawsuits and enforcement actions: (1) be careful of what is said to the public regarding cybersecurity and data privacy, (2) courts seem more willing than not to determine that consumers have suffered "harm" as a result of a cybersecurity incident, (3) both legislative bodies and executive agencies continue to set standards for cybersecurity, and (4) cybersecurity incidents can impact an organization in multiple ways. Suggested actions for organizations to take in light of these trends are included at the end of this document.

---

[1] As an example, take the so-called "Data Valdez" case where AOL allegedly released the search data of 650,000+ users without sufficiently anonymizing the data. The class action was filed in 2006, alleging "The disclosed search data includes sensitive information regarding its members, including their names, social security numbers, addresses, telephone numbers, credit card numbers, user names, passwords, and financial/bank account information. Personal information contained in the search queries can be used to reveal the identity of the AOL member." Appeal was heard in 2010, and AOL finally settled the case in 2013. Later that same year, Target would announce a breach affecting 40 million consumers. See *Doe 1 v. AOL*, 719 F.Supp.2d 1102 (2010), "AOL Settles Data Valdez Lawsuit For $5 Million", Wendy Davis, *MediaPost Publications.* Feb. 19, 2013, and "Target: 40 million credit cards compromised", CNNMoney Staff, *CNNMoney*, December 19, 2013.

Key Takeaways

What you say matters as much as what you do. Even organizations that have not suffered a security breach can get in trouble if they mislead the public as to their cybersecurity practices. An organization should *never* claim cybersecurity certifications not possessed, such as PCI or ISO, nor declare the organization provides a level of cybersecurity that is inaccurate (such as a certain level of encryption). Even a vague statement such as "industry standard security" can get an organization in trouble by inviting challenges to what constitutes "industry standard" in the wake of a breach.

Courts tend to be more willing than not to find consumers have suffered "harm" as a result of a security breach. Although there are some cases to the contrary, as a general trend courts are not willing to dismiss cases on lack of harm. Most organizations should assume that in litigation consumer "harm" will be found, and so the key will be to address that concern before litigation if it all possible.

State and federal governments continue to set standards; determine if these are applicable to your organization. Cybersecurity standards are supposed to evolve as technology evolves. Unfortunately, that evolution is herky-jerky, with stops and starts, and then sudden giant leaps forward. New state and federal standards are not necessarily directly applicable to a particular organization or industry, but governments sometimes *do* give an idea of what is likely to be industry standards in general for any organization. For example, both the Department of Defense and the State of New York have independently set 72 hours as the time for notification of a cybersecurity breach. Consider whether that is now the *de facto* standard for breach notification if the organization is not required to follow some other law or regulation.

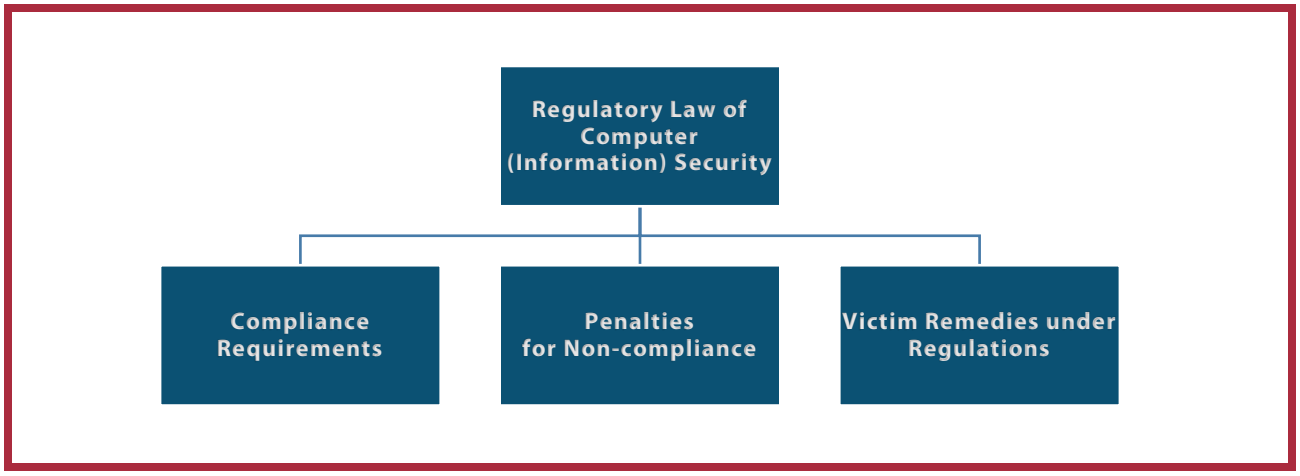
There are many ways for an organization to suffer loss for a cybersecurity breach. Consider what mitigation steps exists and whether these costs, such as cyber liability policies, outweigh the risk of loss from a breach.

Sidebar One: What is "Cybersecurity Law"

"Cybersecurity" has become a ubiquitous term, and an important one for regulated organizations to use when discussing information technology. However, the term itself generally isn't an "official" term; it rarely appears in actual legislation (although that fact is changing). However, there is some risk of confusion if there is no consensus on what "cybersecurity law"[2] actually means.

Focusing on enforcement actions and litigation, there are two areas of cybersecurity law to consider:

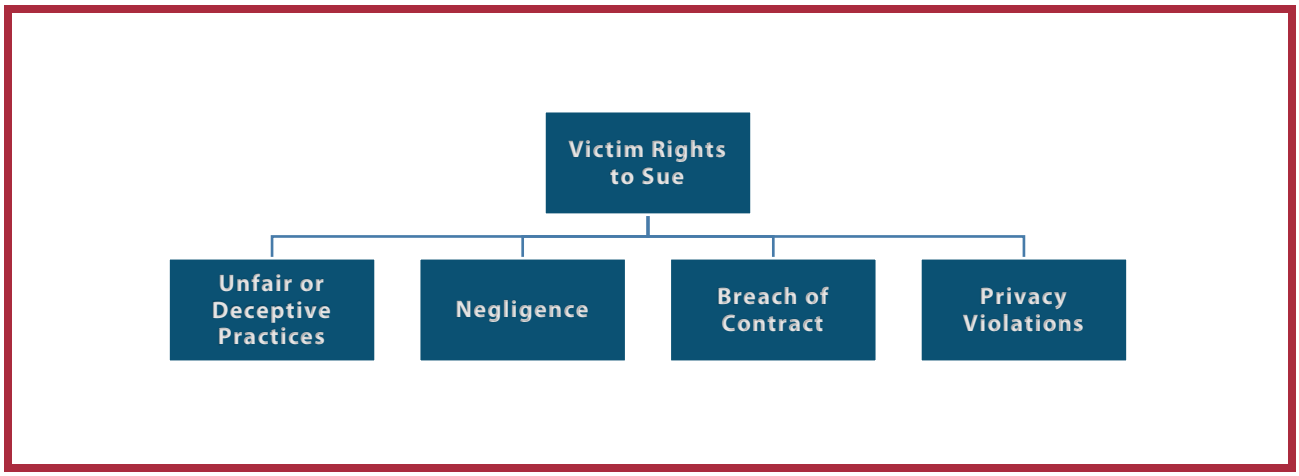
Regulatory law of computer (information) security. Does the law mandate requirements to protect the information and/or privacy of consumers? What are the penalties for non-compliance? Does failure to protect information give the consumer a right to sue due to that failure to protect?



Core elements of regulatory law

Victim rights to sue. Under what legal theory or theories can a victim demand compensation and/or action by an organization that failed to protect consumer information or privacy?

[2] In 2015 *The Washington Post* provided a decent description in an article: "What is 'cybersecurity law'?", Orin Kerr, *The Washington Post,* May 14, 2015.



Core elements of rights to sue

These distinctions aren't always exclusive; in some circumstances, it is possible to be hit with a regulatory action, and *also* be sued by consumers. For example, in 2013 ColorTyme was hit with an FTC action alleging:

> "Since at least October 2008, [ColorTyme] has licensed a software product known as PC Rental Agent from DesignerWare, LLC ("DesignerWare") and installed it on computers it rents to consumers. PC Rental Agent, when installed on a rented computer, enables [ColorTyme] to … remotely install and activate an add-on program called Detective Mode. Using Detective Mode, [ColorTyme] *can surreptitiously monitor the activities of the computer's user, including by using the computer's webcam*. Through Detective Mode, [ColorTyme*] can also secretly gather consumer's personal information using fake software registration windows …* [ColorTyme] *does not tell the computer user about the activation of Detective Mode.*"[3] [emphasis added]

At the same time, ColorTyme was also hit with a class action lawsuit seeking compensatory and punitive damages for violations of the Electronic Communications Privacy Act (ECPA)[4].

However, the truth is most organizations will be victims of cybersecurity breaches, not alleged perpetrators. However, the reality is that even if the organization is a victim, if the organization is responsible for the custody of consumer information the law has an unpleasant habit of making the organization responsible for compensating any victims. Fair or not, an organization that suffers a cybersecurity breach essentially stands in the shoes of the criminal perpetrator when it comes to legal and regulatory liability.

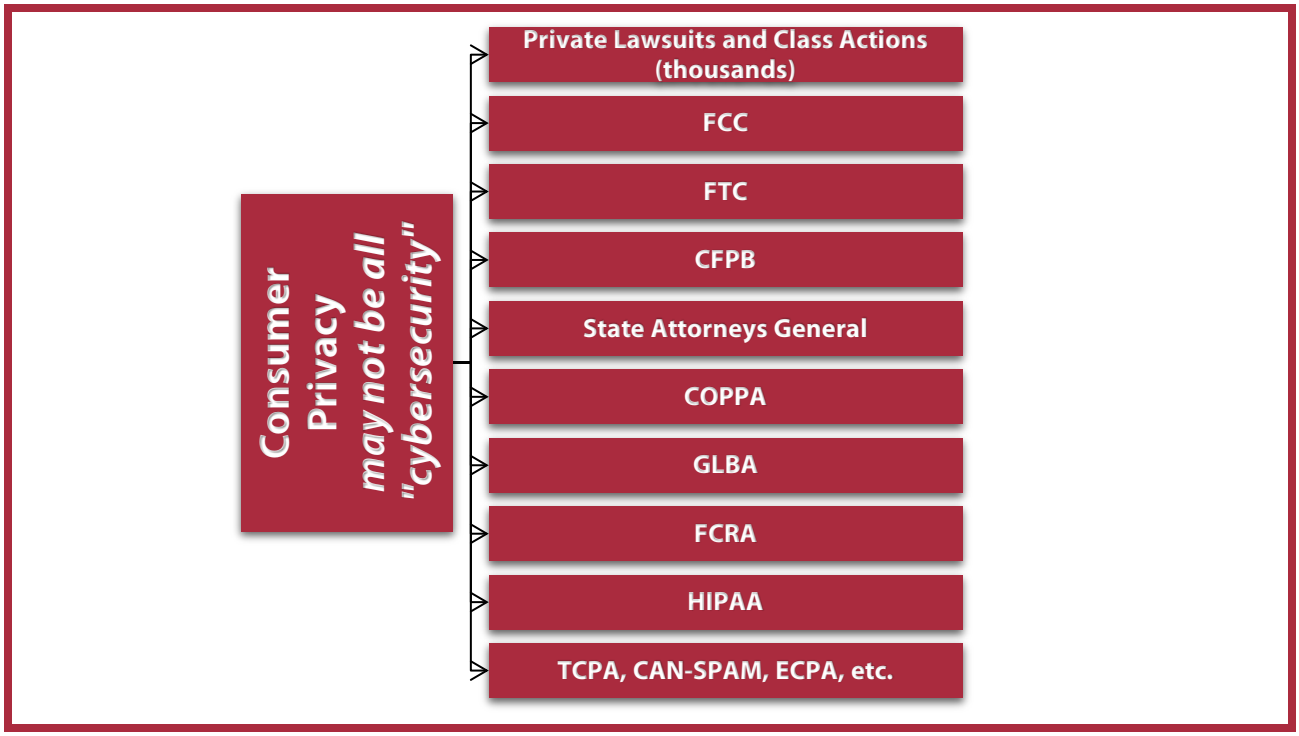
---

[3] *In re J.A.G. Rents, LLC, d/b/a ColorTyme*, Docket No. C-4395, Federal Trade Commission (2013).

[4] See *Arrington v. ColorTyme*, 972 F.Supp.2d 733 (2013).

Sidebar Two: "Hedging" About Compliance

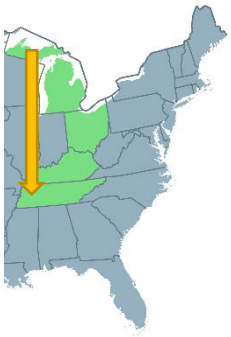
It can be frustrating for an executive to ask for a straight answer from an attorney or compliance officer, and get some version of an "it depends" response. Unfortunately, the right answer is often a complicated one, heavily influenced by the facts and circumstances. For example, when discussing the security of consumer information, the answer might change depending on whether the information involves financial information (GLBA), health information, (HIPAA), children's online privacy (COPPA), and other numerous federal and state laws and regulations related to consumer privacy. Some or all of these may imply questions of cybersecurity, whether around the actual protection of information or the appropriate disclosures to consumers.



A few of the key privacy laws and enforcement actions

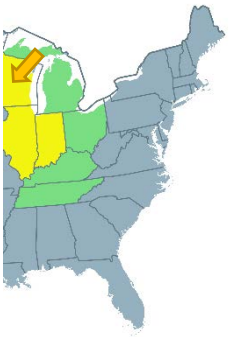
There have been some efforts to help compliance personnel untangle some of these regulations. For example, the State of Minnesota published *A Legal guide to Privacy and Data Security*, which is quite helpful. The document is, however, 164 pages and not exactly light reading for compliance people trying to understand their duties and responsibilities. Even this document hedges by emphasizing there is no single federal data privacy law.

Another, rather odd quirk of the U.S. legal system is the way the federal courts of appeals work. U.S. Federal Appeals Courts are broken down into Circuits. The 6th Circuit, pictured in green, contains the states of Michigan, Ohio, Kentucky, and Tennessee, with the court itself located in Cincinnati. One of the core items to understand is that the rule of a Federal court in one Circuit is binding on all the states within its Circuit but not necessarily any other Circuit.



Upper Peninsula of MI to Tennessee: 800 miles

For example, a 6th Circuit decision that originated in Escanaba, MI affects a company in Memphis, TN, despite being 800 miles away. However, this decision is not binding on the yellow shaded states of the 7th Circuit (Wisconsin, Illinois, and Indiana). Even though the Escanaba, MI company probably has much more in common with Wisconsin companies (and maybe even does business there), and is much less likely to have any contact with Tennessee residents, the decision is binding in Memphis but not Green Bay.

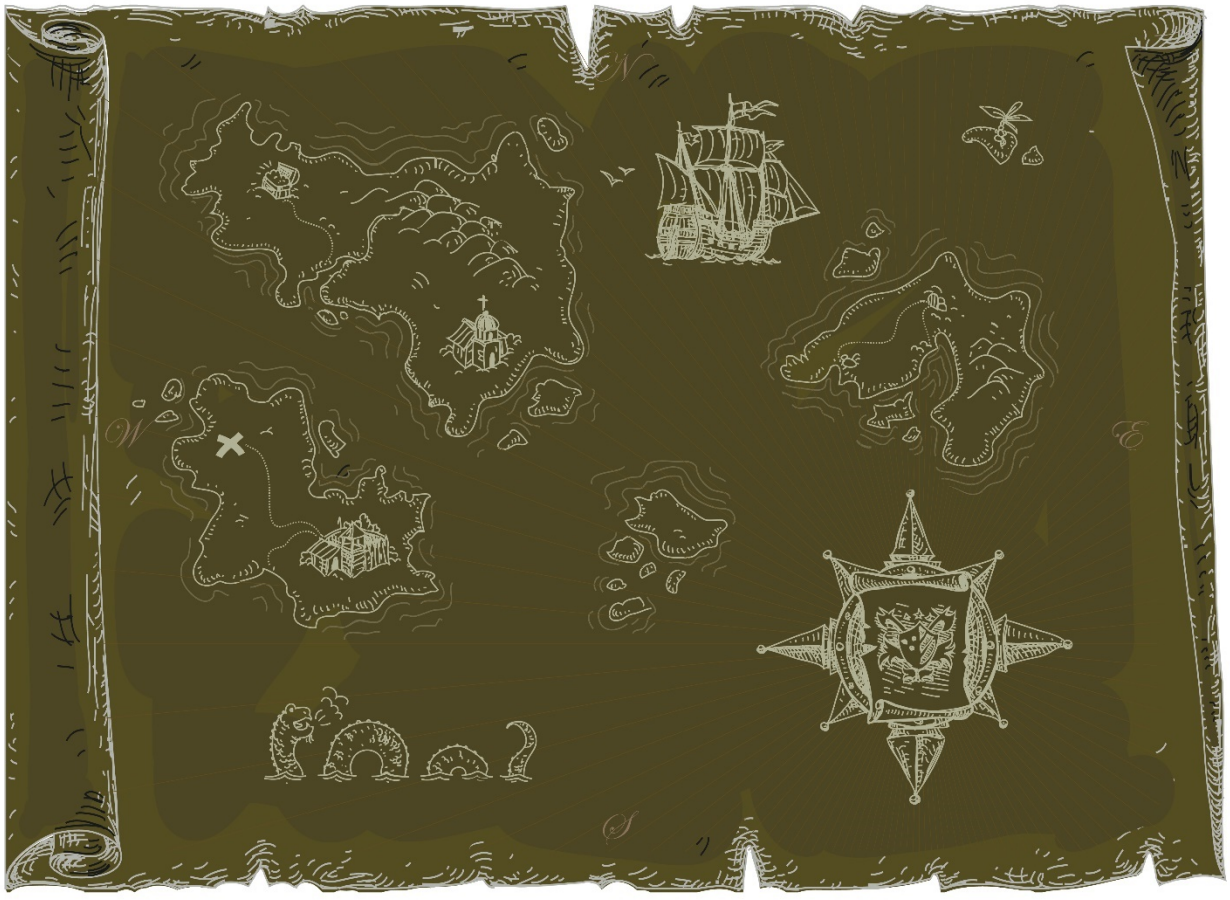


Upper Peninsula of MI to Green Bay, WI: 100 miles

Finally, many cases are settled out of court before a verdict is reached and an appeal heard. This results in a lack of clarity for organizations to follow.

Modern compliance can be a significant challenge for the people assigned to review the regulations. Not only are compliance officers tasked with understanding the text of the regulations, they have to follow the interpretations of federal and state government agencies tasked with enforcement, and also see what is happening in the court system as well. The challenges to stay current are endless.

Here Be Dragons. Good compliance officers will often need to act as scouts for the rest of the team when organization projects or priorities may conflict with existing legislation. Usually, there **is** a way for a project to move forward that maintains compliance with existing laws (although the project may require some redesign in the process). The compliance officer may need to communicate to the rest of the team "**HERE BE DRAGONS**" for dangerous or unexplored activity. The compliance officer is part of the team looking to find a path to success, rather than being an obstacle to the organization's success.



Understand the Opposition

When it comes to cybersecurity issues, there are two possible adversaries for an organization to face: a regulatory agency, or the law firm representing consumers (or both). Therefore, a company facing a breach should be aware of what each potential opponent is looking for when designing internal information security controls and policies.

What an agency is looking for.	**What a plaintiff's counsel is looking for.**
The most serious issue is when a regulatory agency has already noted that the organization is in violation of a statute, and this violation leads to a cybersecurity breach. Another important issue is whether the board and executive officers are kept up to speed on regulatory matters involving cybersecurity. Does cybersecurity information provided to the public or to consumers match up with what the organization's actual practices are? Does the organization use the information it collects unlawfully? *How can the agency show it is protecting the public or fulfilling its statutory authority*[5]?	Counsel wants to be paid, and big money awards are rare in individual cases. Law firms want to file class action lawsuits. In addition, the real money tends not to be due to the hack, but rather the use or misuse of the information exposed. Plaintiff's attorneys are therefore going to look very closely at whether they can make a claim that the organization misrepresented its cybersecurity practices, or worse, collected personal information without the customer's knowledge. Finally, plaintiff's counsel need to demonstrate how consumers were harmed to establish standing and damages.

[5] For example, note the Federal Trade Commission's Press Release regarding settlement of the Wyndham action:

"Wyndham Hotels and Resorts has agreed to settle FTC charges that the company's security practices unfairly exposed the payment card information of hundreds of thousands of consumers to hackers in three separate data breaches.

…

"This settlement marks the end of a significant case in the FTC's efforts to protect consumers from the harm caused by unreasonable data security," said FTC Chairwoman Edith Ramirez. "*Not only will it provide important protection to consumers, but the court rulings in the case have affirmed the vital role the FTC plays in this important area.*" [emphasis added]

"Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk", FTC, December 9, 2015.

Takeaway 1: What You Say Matters

*Of the many topics of interest in cybersecurity law, probably the clearest takeaway is that what an organization says to the public or its consumers **matters**. Misleading the public can be used against the organization in either a class action lawsuit or an enforcement action. If nothing else, every organization that presents privacy information online or in an agreement with the consumer should ensure that this information is accurate and not misleading. Even organizations that have not suffered a security breach can get into trouble if their public privacy information is misleading.*

Avoid Deceptive and Unfair Practices. The key case on this topic is *FTC v. Wyndham Worldwide Corp*. In 2012, the Federal Trade Commission (FTC) filed suit in federal district court against global hotel company Wyndham Worldwide Corporation and its subsidiaries (collectively, "Wyndham") for failing to maintain reasonable and appropriate data security practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." According to the complaint, Wyndham:

> "a. failed to use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems, the Hotels and Resorts' corporate network, and the Internet, such as by employing firewalls;
>
> b. allowed software at the Wyndham-branded hotels to be configured inappropriately, resulting in the storage of payment card information in clear readable text;
>
> c. failed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network;
>
> d. failed to remedy known security vulnerabilities on Wyndham branded hotels' servers that were connected to Hotels and Resorts' computer network, thereby putting personal information held by Defendants and the other Wyndham branded hotels at risk. For example, Defendants permitted Wyndham-branded hotels to connect insecure servers to the Hotels and Resorts' network, including servers using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities;
>
> e. allowed servers to connect to Hotels and Resorts' network, despite the fact that well-known default user IDs and passwords were enabled on the servers, which were easily available to hackers through simple Internet searches;

f. failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess. Defendants did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords. For example, to allow remote access to a hotel's property management system, which was developed by software developer Micros Systems, Inc., Defendants used the phrase "micros" as both the user ID and the password;

g. failed to adequately inventory computers connected to the Hotels and Resorts' network so that Defendants could appropriately manage the devices on its network;

h. failed to employ reasonable measures to detect and prevent unauthorized access to Defendants' computer network or to conduct security investigations;

i. failed to follow proper incident response procedures, including failing to monitor Hotels and Resorts' computer network for malware used in a previous intrusion; and

j. failed to adequately restrict third-party vendors' access to Hotels and Resorts' network and the Wyndham-branded hotels' property management systems, such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary."

According to the FTC, these deficient security practices led to three unauthorized intrusions between 2008 and 2010. These intrusions allegedly caused "the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss.[6]"

The FTC claimed authority to file suit against Wyndham under Section 5 of the Federal Trade Commission Act. A trade practice is *deceptive* if it involves a "material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment." A trade practice is *unfair* if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.[7]"

Wyndham vigorously defended itself, including a major challenge to whether the FTC even had the authority to bring suit for lax data security. The third circuit dismissed Wyndham's objections, and ultimately Wyndham settled with the FTC in 2015. The important language out of the 3rd Circuit opinion:

---

[6] *FTC v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

[7] FTC Act, 15 U.S.C. Sec. 45(a)(1).

> "*A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy*, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.[8]" [emphasis added]

Note no litigation commenced to determine whether Wyndham *actually was* unfair or deceptive. What the Third Circuit said is that the FTC had enough materials in its complaint to charge Wyndham with violations of federal law due to unfair or deceptive trade practices[9].

On the class action side, the case *In re Google, Inc. Cookie Placement Consumer Privacy Litigation*, the Third Circuit actually ended up dismissing most of the plaintiff's state and federal law claims against Google. But the court allowed the claim that Google violated consumer rights to privacy under California law because what Google *said* to consumers conflicted with what Google actually *did* with consumer cookies:

> "What is notable about this case is how Google accomplished its tracking. *Allegedly, this was by overriding the plaintiffs' cookie blockers, while concurrently announcing in its Privacy Policy that internet users could "reset your browser to refuse all cookies*." Google further assured Safari users specifically that their cookie blockers meant that using Google's in-house prophylactic would be extraneous. *Characterized by deceit and disregard, the alleged conduct raises different issues than tracking or disclosure alone.*
>
> …
>
> As the activated cookie blocker equates, in our view, to an express, clearly communicated denial of consent for installation of cookies, we find Google "intru[ded] upon reasonable expectations of privacy."
>
> …
>
> As for whether the alleged conduct is "so serious in nature[ ][and] scope ... as to constitute an egregious breach of the social norms," *Google not only contravened the cookie blockers—it held itself out as respecting the cookie blockers*. Whether or not data-based targeting is the internet's pole star, *users are entitled to deny consent, and they are entitled to rely on the public promises of the companies they deal with* … Particularly as concerns Google's public statements regarding the Safari cookie blocker, we see no justification.

---

[8] *FTC v. Wyndham Worldwide Corp,* 799 F.3d 236 (3d Cir. 2015).

[9] However, the FTC's authority has been challenged elsewhere with the status unresolved.

…

A reasonable jury could conclude that Google's alleged practices constitute the serious invasion of privacy contemplated by California law.[10]" [emphasis added]

Google agreed to settle in 2017[11].

Avoid Misrepresentations to the Public. In 2016, the Consumer Financial Protection Bureau went after eCommerce provider Dwolla, alleging deceptive data security representations. What is interesting in Dwolla, is that the CFPB did *not* allege that Dwolla had actually been breached. Rather, the CFPB claimed that the mere fact that Dwolla was misrepresenting their data security to the public was enough to violate federal law:

"19. On its website or in direct communications with consumers, Respondent made the following representations indicating that its data-security practices met or exceeded industry standards:

a. Dwolla's data-security practices "exceed industry standards," or "surpass industry security standards";

b. Dwolla "sets a new precedent for the industry for safety and security";

c. Dwolla stores consumer information "in a bank-level hosting and security";

d. Dwolla encrypts data "utilizing the same standards required by the federal government."

20. On its website or in direct communications with consumers, Respondent made the following representations regarding its encryption and data-security measures:

a. "All information is securely encrypted and stored";

b. "100% of your info is encrypted and stored securely";

c. Dwolla encrypts "all sensitive information that exists on its servers";

d. Dwolla uses "industry standard encryption technology";

e. Dwolla "encrypt[s] data in transit and at rest";

---

[10] *In re: Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015).

[11] *In re: Google Inc. Cookie Placement Consumer Privacy Litigation*, United States District Court, D. Delaware, (2017).

f. "Dwolla's website, mobile applications, connection to financial institutions, back end, and even APIs use the latest encryption and secure connections"; and

g. Dwolla is "PCI compliant".

…

27. In particular, Dwolla failed to:

a. adopt and implement data-security policies and procedures reasonable and appropriate for the organization;

b. use appropriate measures to identify reasonably foreseeable security risks;

c. ensure that employees who have access to or handle consumer information received adequate training and guidance about security risks;

d. use encryption technologies to properly safeguard sensitive consumer information; and

e. practice secure software development, particularly with regard to consumer facing applications developed at an affiliated website, Dwollalabs."

Dwolla was ordered to stop misrepresenting its data security practices, train employees properly and fix security flaws, and pay a $100,000 civil money penalty[12].

Dragons and how to avoid them. Organizations should be crystal clear the dangers of misrepresenting cybersecurity practices to the public. If an organization engages in misrepresentation, even in the absence of an actual cybersecurity breach, the organization could see regulatory action or class action lawsuits materialize.

If an organization is struggling to define its own cybersecurity statements to the public, one idea is to review those organizations that are under regulatory orders to get a sense of what is acceptable to federal or state regulators. *Not to copy and paste!* Rather, to research and learn from companies that have gone through an unpleasant regulatory experience and derive a feel for what a non-deceptive statement to the public might look like. Organizations should also be careful to review their own public statements to ensure there are no material inaccuracies in what the organization says versus what it does regarding cybersecurity practices.

[12] *In re Dwolla*, File No. 2016-CFPB-0007, Consumer Finance Protection Bureau (2016).

IMPORTANT CASES OR ACTIONS: CONSUMER NOTIFICATION

CASE OR ACTION	YEAR	HEARD BY	ISSUE	KEY HOLDING
FTC. v. Wyndham Worldwide Corp	2015	3rd Circuit	*Misleading Privacy Policy*	A company **does not act equitably** when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.
In re LinkedIn User Privacy Litigation	2014	Northern District of California	*Extra Payment for Security Services Not Rendered*	Plaintiff alleges that LinkedIn used a particular security practice, is specific about what that security practice entailed, alleges that LinkedIn's practice fell below the "bare minimum" security practice in LinkedIn's industry, and plaintiff is specific about what that "bare minimum" security practice entails. Furthermore, **LinkedIn does not contend that the phrase "industry standard" amounts to puffery or is otherwise impossible to define**.
In re Google, Inc. Cookie Placement Consumer Privacy Litigation	2015	3rd Circuit	*False or Misleading Consumer Disclosure*	Users are entitled to deny consent, and **they are entitled to rely on the public promises of the companies they deal with**.
In re Dwolla	2016	CFPB	*False or Misleading Consumer Disclosure*	**Companies may not misrepresent**, expressly or by implication, **the data-security practices implemented by the company**.

Takeaway 2: The Battle for Standing

*Probably the biggest hurdle that a plaintiff's attorney has in making a case against an organization regarding a cybersecurity breach is **standing**. In very basic terms, even if something bad happened and a person's data was stolen, unless that person can show they actually suffered a harm that person lacks "standing to sue[13]."*

Supreme Court seems to create a wall in *Clapper* and *Spokeo*. In 2013, the Supreme Court heard a case (*Clapper v. Amnesty International*) that had nothing to do with cybersecurity but *everything* to do with privacy and standing[14]. The plaintiffs claimed that broad wiretapping powers provided to federal agencies for overseas conversations gave the plaintiffs standing to sue[15]. The Supreme Court said that wasn't enough for standing that this argument "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" The Court went further to add that the plaintiff's "costly and burdensome measures" taken to protect the confidentiality of their communications was not enough for standing[16]. That sounds very much like the kind of case involving cybersecurity.

This sounds great for organizations that have suffered a cybersecurity breach, correct? Indeed, several high-profile data breach cases were thrown out of the trial courts after *Clapper* because the plaintiffs had only alleged harm as a result of the breach, including steps taken to protect their identities or their financial information[17].

In 2016, the Supreme Court heard another case (*Spokeo v. Robins*) where the plaintiff alleged that the defendant, Spokeo, published false information about him online in violation of the Fair

---

[13] To establish Article III standing in federal court, a plaintiff must show an injury-in-fact; a "sufficient causal connection between the injury and the conduct complained of;" and "a likelihood that the injury will be redressed by a favorable decision." (Of course, the devil is in the details here.)

[14] *Clapper v. Amnesty International*, 568 U. S. ____ (2013)

[15] In *Clapper*, the respondents--attorneys and labor, media, and human rights organizations--argued that they had standing based on the "objectively reasonable likelihood" that their sensitive communications with foreign contacts would be monitored under Section 702 of the Foreign Intelligence Surveillance Act. 133 S. Ct. at 1143.

[16] *Clapper*: "… [plaintiffs] cannot manufacture standing *merely by inflicting harm on themselves based on their fears* of hypothetical future harm that is not certainly impending." [emphasis added]

[17] Some of the cybersecurity cases that were dismissed for lack of standing in the wake of *Clapper* included *Galeria v. Nationwide Mutual Insurance Company*, *Strautins v. Trustwave Holdings, Inc.*, *Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, *Remijas v. Neiman Marcus Group, LLC*, *Burton v. MAPCO Express, Inc.*, *Lewert v. P.F. Change's China Bistro, Inc.*, and *Peters v. St. Joseph Servs. Corp*. However, for many of these cases, as will be seen, initial dismissal on standing grounds was not the end of the case.

Credit Reporting Act[18]. The Court once again said that mere allegation of a violation of a statute was not enough; that the plaintiff needed to show that he was somehow harmed by the publication. As an example, the Court noted that if Spokeo published the wrong zip code, it would be hard to see what the harm was to the plaintiff. The case was sent back to the lower courts to determine if under this standard, the plaintiff would actually have standing.

As with *Clapper*, the decision in *Spokeo* appears to be a boon for defendant organizations sued by defendants on the grounds that the plaintiffs are entitled to compensation due to a statute violation (whether caused by a cybersecurity breach or not). The Supreme Court appears to have signaled that there is a losing formula and a winning formula for plaintiffs in a data breach case:

DATA BREACH PLUS STATUTE VIOLATION	**=**	**LOSING FORMULA (USUALLY)**
DATA BREACH PLUS HARM	**=**	**WINNING FORMULA**

But not so fast my friend! Despite the several cases being dismissed in the trial courts due to *Clapper*, many are going right back to trial on appeal. As to be expected, the cases are revolving around to what **harm** is. There are three harms that plaintiffs have been alleging as a result of cybersecurity breaches that have found traction in the U.S. court system:

(a) Actual, specific financial harm (money or identity stolen);

(b) Misuse of information that hasn't been alleged to create actual financial harm; and/or

(c) Alleged risk of the misuse of information (as opposed to actual harm).

Actual harm. Actual specific harm is the easiest way for a plaintiff to avoid dismissal on standing grounds. When plaintiff Sarah Hapka alleged that as a result of the Carecentrix breach someone filed a false income tax report under her name, there was the specific financial harm needed for standing and the negligence claim to proceed (*Hapka v. Carecentrix*[19]).

Another example is *Remijas v. Neiman Marcus Group*. The court here stated that even though 9,200 plaintiffs were later reimbursed for fraudulent charges, these persons still had suffered harm due to having "suffered the aggravation and loss of value of the time needed to set things

[18] *Spokeo, Inc. v. Robins*, 36 S. Ct. 1540 (2016).

[19] Note that Sarah Hapka hasn't obtained money yet, in that she still has to prove that the false income tax return was the result of Carecentrix negligence. *Hapka v. Carecentrix*, Case No. 16-2372-CM, (Kan. D. 2016).

straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges." Here, plaintiff's *incidental costs* were enough to show harm[20].

Misuse of information. The misuse of information is increasingly used by plaintiffs successfully to establish standing, although there is not always consistency among the various courts. The *In re Adobe Systems, Inc. Privacy Litigation* case probably demonstrates the clearest case of when a court will find standing exists. The allegations in *Adobe* included:

- Allegations that the hackers deliberately targeted Adobe's servers;
- Hackers actually collected plaintiffs' personal information;
- Hackers already used Adobe's system to decrypt credit card numbers; and
- Hackers posted some of the information online.

When plaintiffs are able to establish facts such as these, courts seem more willing to provide standing[21]. Adobe Systems settled shortly thereafter.

By contrast, *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, most plaintiffs were found to not have standing after a backup tape containing sensitive information was stolen out of a car. There the court found that for the theft of information to actually cause harm, the thief would have to:

- Recognize what the tapes were;
- Find an appropriate tape reader;
- Attach the tape reader to a computer;
- Acquire software to upload the data from the tapes;
- Decrypt the encrypted portions of the tapes;
- Become familiar with the health insurance company's database format; and
- Misuse a particular plaintiff's name and social security number.

---

[20] *Remijas v. Neiman Marcus Group*, 794 F.3d 688 (7th Cir. 2015).

[21] *In re Adobe Systems, Inc. Privacy Litigation*, 66 F.Supp.3d 1197 (N.D. Cal. 2014).

An interesting twist to the SAIC case is that while most of the class was dismissed, the judge did allow the two plaintiffs' cases to move forward on separate grounds. One plaintiff began receiving unsolicited telephone calls pitching medical products and services targeted at her specific medical condition, a record of which was stored on the tape. The other alleged that he received mail indicating that he had applied for a loan that he did not apply for, and that his credit history had been adversely affected as a result. The court refused to extend these allegations to the class action at large, and also indicated the plaintiffs would still need to demonstrate that the theft of the tape caused the alleged harm[22].

Risk of misuse. *Lewert v. P.F. Chang's China Bistro, Inc.* reinstated a class action case over P.F. Chang's objection that the plaintiffs had failed to show that their data was actually exposed. "At the pleading stage, the plaintiffs' factual allegations must 'cross the line from conceivable to plausible.'[23]" P.F. Chang's could present evidence to contest plaintiff's claims at trial, but at the pleading stage a plausible allegation that their data was stolen and the concrete injury of increased risk of fraudulent charges and identity theft.

In *Galeria v. Nationwide Insurance*, another dismissed case was reinstated even though plaintiffs made no allegations regarding actual incidences of fraud or identity theft. Here, the court said the injury was not hypothetical because Nationwide was targeted by hackers. "Where a data breach *targets* personal information, a reasonable inference can be drawn that *the hackers will use the victims' data for . . . fraudulent purposes . . .* [24]" [emphasis added].

However, a Florida court recently dismissed a case for lack of standing. In *Torres v. The Wendy's Company* the court dismissed the original claims, stating that the plaintiff was reimbursed for his losses through the credit union, and therefore the plaintiffs do not have any claims against Wendy's. The plaintiffs have recently amended their claim to bolster their claim of harm[25].

What's going on here? Plaintiffs in data breach cases have a problem: sue too early, and they have a problem demonstrating they've suffered a harm; sue too late, and the defendant has an argument that harm resulted from some other breach or misuse of their data. (If a plaintiff sues early and as the case drags on they aren't able to show actual injury, they do risk dismissal of the

---

[22] *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation,* 45 F. Supp. 3d 14, 28 (D.D.C. 2014).

[23] *Lewert v. P.F. Chang's China Bistro, Inc.,* 819 F.3d 963 (7th Circuit 2016).

[24] *Galaria v. Nationwide Mutual Insurance Co.*, Nos. 15-3386/3387 (6th Circuit, 2016)

[25] *Torres v. The Wendy's Company*, 6:16-cv-00210, (Fl. Mid. District 2016).

case). The courts appear to be saying, essentially, if you give us enough evidence to plausibly indicate you've suffered harm, we will let the case go forward.

Of course, many plaintiff's attorneys are hoping to get to the trial stage, in the hopes that the expense and possible negative press will force a settlement. Remember too that when judges take off their robes and jurors leave the box, they have credit cards too. They tend to look favorably on keeping cases alive to encourage better security by the organizations with their personal information or at least effective reimbursement of their losses.

Dragons and how to avoid them. In the absence of other direction from the U.S. Supreme Court, it seems that many courts are willing to allow the concept of "harm" to include alleged impending harm. If an organization has a cybersecurity breach, and the questions here can be answered "yes":

> Did hackers specifically target the information?
>
> Did hackers post information online or otherwise misuse the data?
>
> Do consumers have evidence of fraudulent charges?
>
> Is there more harm to the consumer than just the fact that a law may have been violated?

Then the organization are probably looking at a potential class action that has a higher probability of surviving immediate dismissal. Remember, though, whether the case can win on the merits is another question entirely.

Should an organization reimburse or provide monitoring services? Reimbursement doesn't necessarily ensure that the class action will go away, as *Remijas* showed[26]. Indeed, one study found that "overcompensation" may actually hurt brand identity[27]. A consideration would be

---

[26] As expected, the parties settled before trial.

[27] "[Researchers] found that Target customers reacted favorably to a 10-percent discount on purchases. Focusing on three critical outcomes – continued shopping intentions, positive word-of-mouth, and online complaints – the researchers' model showed this form of compensation effectively restored justice perceptions, which had positive effect on customer sentiment.

Another Target strategy – free credit monitoring for affected customers – received mixed reactions. Many customers disliked this strategy, regarding extended periods of free credit monitoring as overcompensation and risking the perception that there was more to the breach than the company communicated.

'Overcompensated customers may feel that the breached organization is not transparent and respectful in its interaction with customers, which leads to low perceptions of justice and poor sentiment,' …"
"Throwing Money at Data Breach May Make It Worse". University of Arkansas. December 22, 2014.

determining the harm or likelihood of harm, and take responsible action to align the response with consumer expectations. This isn't to say that an offer of credit monitoring services wouldn't ever be appropriate, but rather shouldn't be considered the default response[28].

IMPORTANT CASES OR ACTIONS: CONSUMER STANDING TO SUE (HARM)

CASE OR ACTION	YEAR	HEARD BY	ISSUE	KEY HOLDING
Clapper v. Amnesty International	2013	U.S. Supreme Court	*Plaintiff Measures to Protect Against Harm*	Plaintiffs must show harms are "**certainly impending**" — before having standing to sue. Used to dismiss several data breach cases at the lower level.
Spokeo v. Robins	2016	U.S. Supreme Court	*Plaintiff Claims Statute Violation is Harm*	Mere violation of a federal statute **does not automatically confirm standing**; in most cases plaintiffs must show a "concrete injury." This injury does not need to be "tangible" (e.g. a person rejected for a job due to incorrect information posted online *may* have standing).
Hapka v. Carecentrix, Inc.	2016	Kansas Federal District Court	*Actual Harm*	"Key fact" that the plaintiff had suffered an actual, concrete injury: **an individual used her personal information to file a fraudulent tax return shortly after the data breach**. Negligence claim allowed to proceed.
Remijas v. Neiman Marcus Group, LLC	2015	7th Circuit	*Risk of Misuse*	A data breach plaintiff may have standing **based strictly on an alleged impending harm**. The risk of fraudulent charges or identity theft in this instance is ''very real … 'Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur.''
In re Adobe Systems, Inc. Privacy Litigation	2014	Northern District of California	*Risk of Misuse*	Risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is **'immediate and very real**.'"
In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation	2014	D.C. Federal District Court	*Risk of Misuse and Actual Harm*	Only plaintiffs who plausibly alleged that their data was "**accessed or abused**" had asserted the necessary injury-in-fact for standing.

[28] Lynn Sessions, an attorney with the law firm of Baker Hostetler in Houston, … advised that an organization can't notify "until it is ready," meaning until it knows four things: "what happened, how it happened, what the company is going to do for victims, and what the company is going to do to make sure it doesn't happen again." "Hypothetically, Here's How to Respond to a Data Breach". Andrew G. Simpson. *Insurance Journal*. November 13, 2014.

IMPORTANT CASES OR ACTIONS: CONSUMER STANDING TO SUE (HARM)

CASE OR ACTION	YEAR	HEARD BY	ISSUE	KEY HOLDING
Lewert v. P.F. Chang's China Bistro, Inc.	2016	7th Circuit	*Risk of Misuse*	Plaintiffs describe the same kind of future injuries as the *Remijas* plaintiffs did: the increased risk of fraudulent charges and identity theft they face because their data has already been stolen. The Court rejected P.F. Chang's argument that, unlike in *Remijas*, it contested whether the plaintiffs' data was actually exposed in the breach. For the purposes of this lawsuit **that claim is immaterial**. At the pleading stage, the plaintiffs' factual allegations must '[]cross the line from conceivable to plausible.'"
Galaria v. Nationwide	2016	6th Circuit	*Risk of Misuse*	Criminals' deliberate theft of plaintiffs' PII created an immediate, serious and tangible risk that impelled plaintiffs to take protective action**, thereby imposing a concrete and cognizable injury**.
Torres v. The Wendy's Company	2016	Middle District of Florida	*Risk of Misuse*	Plaintiff had no standing because plaintiff had "not alleged any monetary harm stemming from the two fraudulent charges" **nor is the harm "certainly impending**."

Takeaway 3: Agencies and Legislation

With increased cybersecurity focus in both regulatory agencies and in the court system, it should only be expected that state and federal governments are pushing their own standards for cybersecurity compliance. Awareness of these standards can help guide an organization and help with understanding their responsibility for cybersecurity.

Newly Established Cybersecurity Requirements and Guidelines. While not legislation, the Office of the Attorney General for California made the argument that companies doing business in California must, at a minimum, adopt twenty specific security controls established by the Center for Internet Security in order to have "reasonable" security practices in California. The Attorney General's report stated:

"**State Breach Laws**

As the number of state data breach laws has grown in recent years, there has been an effort to pass a federal law that would preempt state laws. The rationale offered has been a reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the bar far below California's current level of protection. They would also in many cases preempt not only state laws on data breach but also longstanding information security and consumer protection statutes.

Recommendations

The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. *The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.*

Organizations should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information. This stronger procedure would provide greater protection than just the username-and-password combination for personal accounts such as online shopping accounts, health care websites and patient portals, and web-based email accounts.

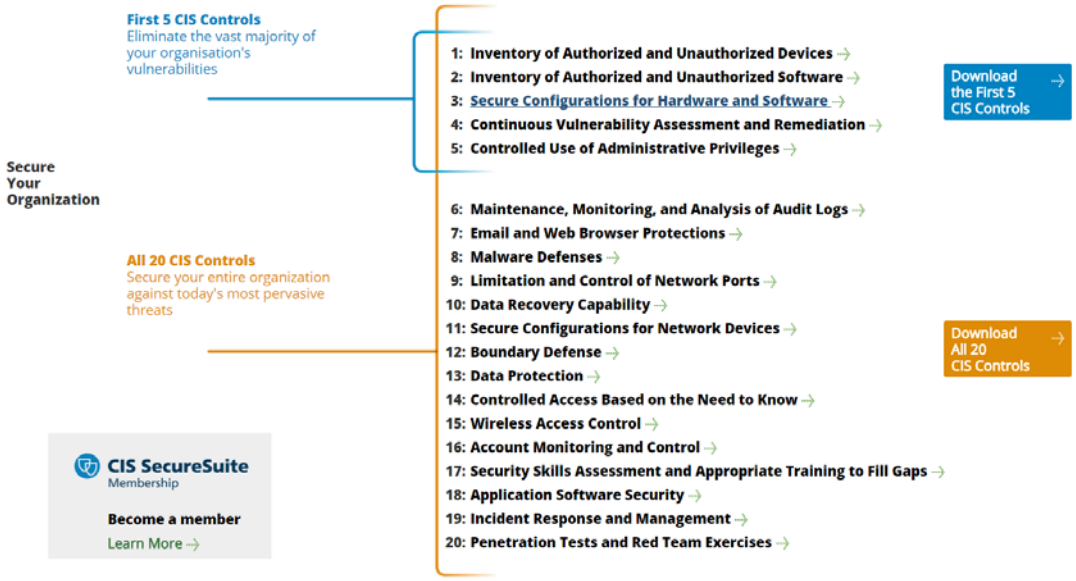
Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers. This is a particular imperative for health care, which appears to be lagging behind other sectors in this regard.

Organizations should encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files and make this option very prominent in their

breach notices. This measure is free, fast, and effective in preventing identity thieves from opening new credit accounts.

State policy makers should collaborate to harmonize state breach laws on some key dimensions. Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections, and retaining jurisdictional expertise.[29]"

What makes the California Attorney General's report more than just a simple recommendation is that California Civil Code § 1798.81.5 requires all businesses that collect personal information on California residents to use "reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure." However, to date the California Attorney General's office has not sued an entity for failure comply with the CIS controls.



Center for Internet Security Controls[30]

On the other side of the country, the State of New York has established several mandatory cybersecurity requirements for financial services institutions (institutions that are regulated by

[29] "California Data Breach Report". Kamala D. Harris, Attorney General, California Department of Justice. February 2016.

[30] "CIS Controls". Center for Internet Security.

New York banking, insurance, or financial services laws) that took effect March 2017. The core aspects of this law include:

Personnel. Entities must designate a qualified individual to act as a chief information security officer (CISO), responsible for developing and presenting a written report to the board of directors on at least an annual basis. The CISO can be employed by an affiliate or third party service provider.

Reporting obligations. If there is an act or attempt to gain unauthorized access to information, the entities may need to report to the State of New York within 72 hours. Also, by 2018 the chairperson of the board of directors must report that its cybersecurity program complies with New York's regulations. This implies personal liability to the chairperson for non-compliant reports.

Documentation obligations. All documentation and information relevant to its cybersecurity program must be made available to the available to the New York Department of Financial Services.

Third party service providers. All entities must address security concerns with third parties that have access to Nonpublic Information, including contractual protections[31].

The State of New York has not yet sued for enforcement of these regulations against an organization doing business in New York. At this time, no other state has passed mandatory cybersecurity regulations similar to California and New York, although several states made different proposals in 2016 for additional cybersecurity regulation.

Federal changes and considerations. At the federal level, the Department of Defense now requires it contractors to implement specific cybersecurity controls and requires notification of cybersecurity incidents within 72 hours. These requirements may soon be the model for all federal agencies.

The FFIEC created its Cybersecurity Assessment tools in 2015, although that toolset has come under increasing fire for not being aligned with current cybersecurity standards (e.g. the National Institute of Standards and Technology's cybersecurity framework), being too labor intensive, and being used by examiners despite the statement that use of the tool is voluntary.

---

[31] "23 NTCRR 500 Cybersecurity Requirements for Financial Services Companies". New York State Department of Financial Services.

Congress as usual has been busy, proposing at least ten bills involving some kind of cybersecurity regulation. For example, the Securing IoT Act of 2017 would require equipment using certain frequencies to meet new cybersecurity standards, defined by the FCC and NIST. The Interagency Cybersecurity Cooperation Act would require a new interagency committee to look at security reports as they purport to telecom, and produce recommendations to be sent to Congress and/or other government departments as required. The Cybersecurity Responsibility Act, would require rules on how to secure communication networks, as well as define them as critical infrastructure. While it is unlikely that any of these proposed bills will become law, this is a reminder that Congress does have interest in cybersecurity legislation. A major security event or other issue might cause one or more of these bills to become law[32].

Dragons and how to avoid them. Ever since federal legislation such as Gramm-Leach-Bliley (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) were promulgated[33], the question has been "Where has the bar for minimum (or "reasonable" or "commercially reasonable" security been set?" For example, in 2000, the idea of encryption to secure information[34] was relatively unknown to the general public. Now, encryption is commonplace (even lawyers and judges use it!).

So even if the organization is not directly impacted by these regulations or legislation, it is a very good idea to look and see where the standards are now and where they are heading. For example, no one can say for certain whether the State of New York's and the Department of Defense's requirements of 72 hours-notice with respect to a cybersecurity incident is a new "standard," but the fact that two different agencies are using the same time frame is indicative that this is where the trend is heading. Applying this knowledge can help protect against an accusation that an organization is not following appropriate "standards" or "best practices."

[32] For example, a highly-publicized event of a self-driving car that is hacked and used as a murder weapon.

[33] In the late 1990s!

[34] Fun fact: GLBA does not mention the word "encryption" anywhere in the legislation.

Takeaway 4: Other Cybersecurity Issues

These are key quick hitters to be aware of.

Successful cybersecurity lawsuits. There are three fundamental ways in which consumers have been successful against organizations that have had a cybersecurity breach. These are cases where there is no real question of harm, but rather how the plaintiff can successfully sue for damages.

> **Violation of statute or regulation**. The defendant bank was found to be in violation of the Uniform Commercial Code by having "commercially unreasonable" security. The bank flagged fraudulent transactions as suspect but did not notify the consumer or block the transfers[35].
>
> **Breach of contract**. Defendant had an implied contract that it would take "reasonable measures[36]" to protect security, but hackers stole 4.2 million debit and credit card numbers.[37]
>
> **Negligence**. Plaintiffs were allowed to continue on a negligence theory based on defendant's massive data breach[38].

Financial institutions going after the retailers. There is an increasing number of cases where financial institutions, after bearing the cost to reimburse card holders for losses incurred during a data breach, are turning around and suing the retailer. Home Depot agreed to settle for $25 million, Target proposed a $10 million settlement with financial institutions and another $20 million to MasterCard, and Wendy's is also facing a class action from credit unions and banks for their alleged data breach.

FCC has also gone after companies for lax cybersecurity. In 2014, the FCC followed the FTC's lead and alleged two companies had "unjust and unreasonable practice" for inadequately protecting the information and failing to notify customers, as well as "deceptive and misleading"

---

[35] *Patco Const. Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012).

[36] *Anderson v. Hannaford Brothers*, 659 F.3d 151 (1st Cir. 2011).

[37] Google is facing the possibility of a class action for breach of the implied covenant by alleging that Google violated its "obligation not to disclose [users'] personal information except as necessary to a transaction or as otherwise specifically authorized." If successful, this could open the door for similar contract-based lawsuits. *Svenson v. Google Inc., et al., No. 5:13-cv-04080, N.D. Calif.).*

[38] *Lone Star Nat. Bank v. Heartland Payment Systems*, 729 F. 3d 421 (5th Circuit, 2013).

representations contained in the two companies' privacy policies[39]. The FCC has since backed off somewhat on regulating cybersecurity and in 2017, the House of Representatives rejected proposed FCC privacy regulations.

SEC also gets involved. In 2016 Morgan Stanley paid a $1 million fine to settle U.S. Securities and Exchange Commission civil charges that security lapses at the Wall Street bank enabled a former financial adviser to tap into its computers and take client data home. The former adviser, Galen Marsh's, transferred without authorization data from about 730,000 accounts to his home computer in New Jersey, some of which was hacked by third parties and offered for sale online[40].

Mergers and acquisitions. While not leading directly to litigation, Verizon's 2016-2017 acquisition of Yahoo! for over $4 billion hit a major snag after the revelation that Yahoo! suffered a hack that may have exposed as many as one billion users. Although the merger eventually went through, Yahoo! was forced to reduce its sales price by an estimated $350 million.

Privacy invasions lead to accusations and litigation. Companies that are accused of surreptitiously collecting private data tend to find themselves in court. In one case, Vizio was accused of violating the Video Privacy Protection Act and California state law for surreptitious monitoring of TV viewing and accessing home networks[41]. Another case accused Facebook of violating the Illinois Biometric Protection Act by improperly collecting biometric (face recognition) data[42]. Lenovo is facing litigation under the Electronic Communications Privacy Act and the Stored Communications Act for inserting software on laptops[43].

Cybersecurity breaches can lead to shareholder action. After the 2013 Target point of sale breach, shareholders filed suit against executive officers and the Board for breach of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control[44]. As with many shareholder derivative actions coming out of cybersecurity[45], the suit was dismissed in 2016. However, organizations should be aware that the possibility of shareholder action does exist.

---

[39] *In re TerraCom, Inc. and YourTel America*, Inc.EB-TCD-13-00009175, Federal Communications Commission (2014).

[40] Marsh faced criminal charges, but avoided jail time with a sentence of three years' probation and $600,000 in restitution after pleading guilty to one felony count of unauthorized access to a computer. "SEC: Morgan Stanley Failed to Safeguard Customer Data," SEC, June 8, 2016.

[41] *In re Vizio, Inc., Consumer Privacy Litigation,* 8:16-ml-02693-JLS-KES, C.D. CA (2017).

[42] *In re Facebook Biometric Information Privacy Litigation,* 3:2015cv03747 N.D. CA (2015).

[43] *In re: Lenovo Adware Litigation*, case number 5:15-md-02624, N.D. CA (2016).

[44] *Collier v. Steinhafel*, No. 14-cv-00266-PAM-JJK, D. Minn (2014).

[45] Wyndham Hotels and Heartland Payment Systems also had dismissed shareholder lawsuits after data breaches.

Class certification. The case involving the Target POS breach had an interesting take not on standing but on class certification in a class action lawsuit. There was a class conflict among the plaintiffs; while *all* of the plaintiffs alleged their data was stolen, only *some* could show harm and be entitled to compensation, but all plaintiffs were forced to accept the class action settlement. This conflict disrupted the settlement process for Target[46]. The lesson here is that if a defendant organization is going to settle, *they should not include class members who have no possibility of being compensated under the settlement*.

FTC too aggressive? In 2005, a small medical testing company called LabMD allegedly accidentally shared the billing details of 9,000 clients in a peer-to-peer file sharing network. In addition, at least 500 of the company's consumers were allegedly exposed to identity thieves in 2012. These issues led to an FTC enforcement action, the costs of defending which allegedly bankrupted the company. Initially, the FTC's own Administrative Law Judge determined that the FTC was overreaching its authority, but in 2016 the FTC vacated that decision and unanimously declared LabMD's actions were "unfair" under Section 5 of the FTC Act.

However, in November, 2016 the Eleventh Circuit heard the appeal of LabMD, and reversed the FTC stating that the FTC's interpretations its data security authority were likely not reasonable[47]. This could lead to a split between the Third Circuit and the Eleventh Circuit, and might cause the Supreme Court to intervene and review the FTC's jurisdiction.

Insurance items. There is no immediate clarity as to whether a commercial general liability policy will cover an organization for cybersecurity events. In 2015, a New York trial court ruled Zurich Insurance was not obligated to defend Sony against the class action lawsuits stemming from the infamous Sony PlayStation Network breach[48]. The parties settled in 2015. However, in 2013 a California court *did* find a duty for an insurer to defend a hospital from a data breach lawsuit[49].

As the nascent market for cyber insurance grows, litigation is starting to crop up as to what is actually covered by the policy. For example, in the P.F. Chang's data breach, P.F. Chang's credit card processor Bank of America Merchant Services ("BAMS"), incurred approximately $1.9 million in costs as a result of the breach. Costs included notification, new cards, and covering fraudulent charges. P.F. Chang's reimbursed BAMS and then sought coverage under its cyber

---

[46] *In re: Target Corporation Customer Data Security Breach Litigation*, Nos. 15-3909, 15-3912, 16-1203, 16-1245, 16-1408, (8th Circuit 2017).

[47] *LabMD v. FTC*, No. 16-16270, (11th Circuit 2016).

[48] *Zurich American Insurance Company v. Sony Corporation of America,* 127 A.D.3d 662 (2015).

[49] *Hartford Casualty Insurance Co. v. Corcino & Associates*, CV 13-03728-GAF (C.D. Cal. Oct. 7, 2013).

insurance policy provider, Federal Insurance. Federal Insurance won the initial round with a finding that P.F. Chang's had no reasonable expectation that its policy would cover such costs, and that P.F. Chang's could have specifically negotiated for such coverage[50]. The case is currently on appeal.

In contrast, the State Bank of Bellingham won a case against BancInsure when BancInsure denied a claim related to a criminal hack because of employee negligence. The Eighth Circuit found that "even if the employees' negligent actions "played an essential role" in the loss and those actions created a risk of intrusion into Bellingham's computer system by a malicious and larcenous virus, the intrusion and the ensuing loss of bank funds was not "certain" or "inevitable." The "overriding cause" of the loss Bellingham suffered remains the criminal activity of a third party[51]."

For most organizations, it is best to inquire directly of its insurers as to what is covered and what is not in the event of a data breach.

Dragons and how to avoid them. There are, as can be expected, many dragons circling around issues with cybersecurity and data privacy. Fundamental items to consider are:

> **Contractual promises**. Are the contracts with consumers either expressly or implied to provide a level of cybersecurity that does not actually exist?
>
> **Reasonable security**. Is the organization keeping up with the latest trends in "reasonable" or "commercially reasonable"[52] security?
>
> **Be aware of other regulatory bodies**. Other regulatory bodies, not just the organization's primary regulator, may be able to take action against an organization that had a cybersecurity breach. Has the organization considered what other regulators may be able to do in the event of a breach?
>
> **Mergers and acquisitions**. Acquiring organizations need to have a plan for potential cybersecurity breaches in the acquired company. Will the acquiring company inherit the liability? Does the potential acquisition have insurance that will cover the acquiring company? How will cybersecurity breaches be communicated?

---

[50] *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, No. 15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. 2016).

[51] *State Bank of Bellingham v. BancInsure, Inc.*, No. 14-3432, --- F.3d ---, 2016 WL 2943161 (8th Cir. May 20, 2016).

[52] Essentially, "commercially reasonable" compares organizations of similar sizes and customer bases to determine what is "reasonable" for similar businesses. For example, if every financial institution in a metro area uses encrypted communications except one, that financial institution could be liable from a breach resulting from the lack of encryption.

Think carefully about consumer rights to privacy. Collecting information about consumers without their consent tends to be extremely unpopular. Has the organization considered how to disclose to consumers about data collection, and what rights the consumer may have to opt out? Does the organization really need this information, or if needed can it dispose of the information?

Shareholder actions. Although usually not successful, shareholders may go after senior officers and the board for cybersecurity breaches. Has the organization ensured that senior management has been provided with the necessary information regarding the organization's cybersecurity posture?

Insurance for cyber events. Does the organization understand what is covered, and more importantly what is *not*, in a cyber event?

IMPORTANT CASES OR ACTIONS: OTHER ITEMS

CASE OR ACTION	YEAR	HEARD BY	ISSUE	KEY HOLDING
Patco Constr. Co., Inc. v. People's United Bank	2012	1st Circuit	*Statute Violation*	Defendant may have violated the UCC by **ignoring multiple warnings from its own security system** that the fraudulent transactions were high risk; consumer was not notified.
Anderson v. Hannaford Brothers	2011	1st Circuit	*Contract Violation*	Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that **an implicit agreement to safeguard the data is necessary to effectuate the contract**.
Lone Star Nat'l Bank v. Heartland Payment Systems	2013	5th Circuit	*Negligence*	We hold therefore that **a defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages**, aside from physical injury, to particular plaintiffs or plaintiffs comprising an identifiable class with respect to whom defendant knows or has reason to know are likely to suffer such damages from its conduct.
In re Matter of TerraCom, Inc. and YourTel America, Inc.	2014	FCC	*Regulatory Violation*	FCC found defendants **apparently willfully and repeatedly violated Sections 201(b) and 222(a) of the Communications Act of 1934** by failing to protect consumer data.
SEC v. Morgan Stanley	2016	SEC	*Regulatory Violation*	Morgan Stanley's **policies and procedures were not reasonable** … that allowed its employees to access customers' confidential account information. Morgan Stanley also did not monitor or analyze employees' access to and use of the [information].

CASE OR ACTION	YEAR	HEARD BY	ISSUE	KEY HOLDING
In re Vizio, Inc., Consumer Privacy Litigation	2017	Central District of California	*Violation of VPPA*	The Video Privacy Protection Act provides that "[a] video tape service provider who **knowingly discloses**, to any person, **personally identifiable information** concerning any consumer of such provider **shall be liable to the aggrieved person**…"
In re Facebook Biometric Information Privacy Litigation	2016	Northern District of California	*Violation of BIPA*	BIPA regulates the collection, retention, and disclosure of personal biometric identifiers and biometric information. Plaintiffs allege that Facebook scans user-uploaded photographs to create a "**unique digital representation of the face ... based on geometric relationship of their facial features**."
In re Lenovo Adware Litigation	2016	Northern District of California	*Violation of ECPA; Actual Harm*	Plaintiffs in the instant case allege that defendants' **privacy violations and the resulting decreased performance actually happened**.
Collier v. Steinhafel	2016	District of Minnesota	*Shareholder Action*	A Special Litigation Committee concluded that it would not be in Target's best interests to pursue claims against the officers or directors.
In re Target Data Breach Litigation	2017	8th Circuit	*Class Certification*	Defendant may not be able to settle with members of a class action who suffered no damage as a result of the data breach, but might in the future. **Plaintiffs who stand to receive nothing under the settlement but are nonetheless required to release future claims may need to be a separate class requiring a separate settlement**.
FTC v. LabMD	2016	11th Circuit	*FTC Statutory Authority*	The court reads both "probable" and "reasonably expected," to require a higher threshold than that set by the FTC. In other words, we do not read the word "likely" to include something that has a low likelihood. **We do not believe an interpretation that does this is reasonable.**
Zurich American Insurance Company v. Sony Corporation of America	2014	New York Supreme Court	*Insurance*	The term "Oral or written publication, in any manner, of material that violates a person's right of privacy" **did not afford coverage for either a defense or indemnity in Sony's favor** in connection with the underlying complaints.
Hartford Cas. Ins. Co. v. Corcino & Associates	2013	Central District of California	*Insurance*	Court rejected Hartford's efforts to escape coverage. **Rights at issue were** not created by statute but have instead been **long recognized under common law**.
State Bank of Bellingham v. BancInsure, Inc.	2016	8th Circuit	*Insurance*	Even if the employees' negligent actions "played an essential role" **the "overriding cause" of the loss Bellingham suffered remains the criminal activity of a third party."**

Practical Cybersecurity Checklist

Deceptive and Unfair Trade Practices (statements to the public).

Review all public cybersecurity statements by the organization for errors or misleading statements, especially claims about cybersecurity that are false.

Research the public cybersecurity statements of companies that have been the subject of regulatory action (do not copy and paste!).

Harm to consumers as the result of a cybersecurity breach.

Evaluate the severity of a cybersecurity breach based on the likely harm to consumers.

Prepare a plan to respond to a cybersecurity breach based on disclosing what happened, how it happened, with the organization will do for victims, and remediation steps the organization will take.

New legislation or proposals by government agencies.

Review the implemented standards of the agencies or of the legislation and determine whether these standards are applicable to the organization's own cybersecurity program.

Other important cybersecurity items to review.

Review contracts with consumers to determine whether the organization is actually meeting its cybersecurity requirements.

Determine if the organization has "reasonable" cybersecurity.

Ensure the organization is prepared for all regulatory authorities that may take an interest in the organization's cybersecurity.

Be sure the organization does appropriate due diligence with cybersecurity when engaging in mergers or acquisitions.

Be sure the organization properly discloses to consumers when it collects information.

Ensure executive management and the board have adequate materials to make informed cybersecurity decisions.

Review insurance for cybersecurity events, and understand the coverage and exclusions.

Historical Class-Wide Settlements of Data Breach Claims

Columbia Law School published a chart detailing cybersecurity data breach settlements. The chart reflects the relevant defendant, the date of final approval of the class-wide settlement, the data type involved in the data breach, the relief provided to the class as part of the settlement, and any fees and costs awarded to class counsel and service awards ordered for class representatives.

DEFENDANT	APPROVAL	DATA TYPE	RELIEF TO THE CLASS	SERVICE AWARDS, FEES, & COSTS
Home Depot (Consumer Class)	August 23, 2016	Card Data	Up to $13 million for class claims; up to $6.5 million for 18 months of credit monitoring services; security practices changes	$1,000 for each representative plaintiff; $166,925 in costs; $7.536 million in fees
Target (Financial Institution Class)	May 12, 2016	Card Data	Up to $20.25 million for class claims; $19.108 million to MasterCard	Reportedly up to $67 million for Visa's claims against Target; $20,000 for 5 representative plaintiffs; $2.109 million in costs; $17.8 million in fees
Sony	April 6, 2016	Login and Personal Information	Up to $2 million for preventative losses; up to $2.5 million for claims for identity theft losses; up to two years of credit monitoring services	$3,000 for each named plaintiff; $1,000 for each plaintiff who initially filed an action; $2.588 million in fees
St. Joseph Health System	February 3, 2016	Health Information	$7.5 million in cash payment; up to $3 million for class claims; one year of credit monitoring services (offered during remediation); security practice changes	$50,000 in incentive payments for class representatives; $7.45 million in fees and costs
Target (Consumer Class)	November 17, 2015	Card Data	Up to $10 million for claims; security practice changes	$1,000 for three deposed plaintiffs; $500 for other plaintiffs; $6.75 million in fees

DEFENDANT	APPROVAL	DATA TYPE	RELIEF TO THE CLASS	SERVICE AWARDS, FEES, & COSTS
LinkedIn	September 15, 2015	Login Information	Up to $1.25 million for claims; security practice changes	$5,000 for the named plaintiff; $26,609 in costs; $312,500 in fees
Adobe	August 13, 2015	Login and Card Data	Security practice changes and audit	$5,000 to each individual plaintiff; $1.18 million in fees
Sony Gaming Networks	May 4, 2015	Card Data and Personal Information	Up to $1 million for identity theft losses; benefit options including free games and themes or month subscription, unused wallet credits, virtual currency; some small cash payments	$2.75 million in fees
AvMed	February 28, 2014	Personal Information	Up to $3 million; security practice changes	$5,000 for each representative plaintiff; $750,000 in fees
Purchasing Power (Winn-Dixie)	October 4, 2013	Personal Information	Up to $225,000 for class claims; up to one year of credit monitoring services; security practice changes	$3,500 for representative plaintiff; $200,000 in fees
CBR Systems	July 24, 2013	Health Information	Up to $500,000 for claims for expenses; up to $2 million for class claims for identity theft; two years of credit monitoring services; security practice changes	$5,000 for representative plaintiff; $14,064 in costs; $585,936 in fees
Michaels Stores (Pin Pad Litig.)	April 17, 2013	Card Data	Up to $800,000 for class claims; up to two years of credit monitoring services; security practice changes	$2,500 for each representative plaintiff; $55,565 in costs; $1.2 million in fees
Heartland Payment Systems	March 20, 2012	Card Data	Up to $2.4 million for class claims; security practice changes	$35,000 in costs; $606,193 in fees
Countrywide	August 23, 2010	Personal and Financial Information	Up to $5 million for claims for identity theft; up to $1.5 million for claims for expenses; two years of credit monitoring services	$500 for each representative plaintiff; $250 for each named plaintiff; $100,000 in costs; $3.5 million in fees

DEFENDANT	APPROVAL	DATA TYPE	RELIEF TO THE CLASS	SERVICE AWARDS, FEES, & COSTS
Dep't of Veterans Affairs	September 23, 2009	Personal Information	Up to $20 million for class claims	$18,000 for representative plaintiffs; $157,076 in costs; $3.6 million in fees
Certegy Check Services	September 3, 2008	Card Data	Up to $4 million for claims for identify theft; up to $1 million for claims for expenses; up to two years of credit monitoring services; security practice changes	$500 for some representative plaintiffs; $250 for each other named plaintiff; $2.35 million in costs and fees
TJX	September 2, 2008	Card Data and Driver's License Information	License replacement cost; up to $1 million for >$60 identity theft; up to $30 in cash; up to three years of credit monitoring services; up to $7 million in vouchers up to $60; one-time 15% discount event; security practice changes	$6.5 million in fees

Resources

Cybersecurity Resources (General)

"A Legal Guide to Privacy and Data Security". Minnesota Department of Employment and Economic Development; Gray Plant Moody. (PDF)

"App developers should beware of the risks associated with transmitting data from a user's mobile device to external servers". Porter Wright. Technology Law Source. January 6, 2015.

"CIS Controls". Center for Internet Security.

"Dwolla Privacy Policy". Dwolla. January 10, 2017.

"GLBA Compliance: U-M Financial Services Information Security Plan". University of Michigan.

"23 NTCRR 500 Cybersecurity Requirements for Financial Services Companies". New York State Department of Financial Services.

"Safeguards Rule". FTC.

"What is 'cybersecurity law'?". Orin Kerr. *The Washington Post*. May 14, 2015.

Class Standing in Cybersecurity Cases

'Target Data Breach Settlement: Eighth Circuit Orders Trial Court To Reconsider Class Certification". John E. Goodman, Michael R. Pennington, J. Thomas Richie. *Bradley Insights and Events*. February 3, 2017.

Consumer Restitution Issues

"Hypothetically, Here's How to Respond to a Data Breach". Andrew G. Simpson. *Insurance Journal*. November 13, 2014.

"So what does a corporation owe you after a data breach?". David Lazarus. *Los Angeles Times*. May 10, 2016.

"Throwing Money at Data Breach May Make It Worse". University of Arkansas. December 22, 2014.

Cyber Liability Insurance Issues

"Policyholder Data Breach Covered Despite "Essential" Employee Negligence". Jennifer E. White. *Hunton Insurance Recovery Blog*. May 31, 2016.

"Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York". Young Ha. *Insurance Journal*. May 1, 2015.

Government Cybersecurity Enforcement Actions

"CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices". CFPB. March 2, 2016.

"FTC v. Wyndham Worldwide Corp.: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability". Harvard Law Review. February 10, 2016.

"FTC v. Wyndham: Whether the Federal Trade Commission Has the Authority Under Section 5 of the FTC Act to Bring an Enforcement Action Against a Company Whose Failure to Protect Sensitive Data Has Resulted in Financial Harm to Consumers". epic.org.

"Morgan Stanley pays $1 million SEC fine over stolen customer data". Jonathan Stempel. *Reuters*. June 8 2016.

"TERRACOM AND YOURTEL TO PAY $3.5 MILLION TO RESOLVE CONSUMER PRIVACY & LIFELINE INVESTIGATIONS". FCC. (PDF)

"The FTC and the New Common Law of Privacy". Daniel J. Solove and Woodrow Hartzog. Columbia Law Review (2014).

"Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk". FTC. December 9, 2015.

Legislation and Other Regulatory Documentation Regarding Cybersecurity

"California Data Breach Report". Kamala D. Harris, Attorney General, California Department of Justice. February 2016.

"Cybersecurity Assessment Tool". FFIEC.

"Cybersecurity Legislation 2016". National Conference of State Legislatures. December 8, 2016.

"New York Cybersecurity Regulations for Financial Institutions Enter Into Effect". Michael Krimminger. *Harvard Law School Forum on Corporate Governance and Financial Regulation*. March 25, 2017.

"Defense Cybersecurity Requirements: What Small Businesses Need To Know". Office of Small Business Programs, U.S. Department of Defense. (PDF)

Merger and Acquisitions Involving Cybersecurity Incidents

"Guest Post: Three Cybersecurity Lessons From Yahoo's Legal Department Woes". Kevin M. LaCroix. *The D&O Diary*. March 30, 2017.

"Three Lessons All Companies Can Learn from the Data Breaches that Cost Yahoo $350 Million". JDSupra. March 16, 2017.

Overview of Cybersecurity Laws and Events

"2016 Cybersecurity Year in Review, and Data Privacy Trends to Watch in 2017". *The National Law Review*. Thursday, January 5, 2017.

"5 Cybersecurity Mistakes that Lead to Regulatory and Legal Action". Michelle A. Reed and Jay K. Tatachar. *Risk Management*. October, 2016.

"A Primer on Cybersecurity Litigation for the Not-So-Tech-Savvy Attorney". Saundra McDavid. *ABA*. March, 2014.

"Cybersecurity Litigation: Where We've Been and Where We're Going". *ABA*. April 13-15, 2016. (PDF)

"Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy". Alexander H. Southwell, Eric Vandevelde, Ryan Bergsieker and Jeana Bisnar Maute. *The CLS Blue Sky Blog*. February 3, 2017.

"Privacy Developments: Private Litigation, Enforcement Actions, Legislation, and Administrative Actions". John Black and James Steel. *The Business Lawyer; Vol. 72, Winter 2016–2017*.

Retailer Liability to Financial Institutions for Cybersecurity Breaches

"EVERYTHING YOU NEED TO KNOW ABOUT THE TARGET DATA BREACH LAWSUITS". Kaleigh Simmons. *RIPPLESHOT BLOG*. February 4, 2015.

"Home Depot Will Pay $25 Million To Banks, Credit Unions Over 2014 Data Breach". Chris Morran. *Consumerist*. March 9, 2017.

"Michigan credit unions join lawsuit over Wendy's credit card data breach". Brad Devereaux. *MLive*. July 31, 2016.

Shareholder Actions for Cybersecurity Breaches

"Shareholders Sue Companies For Lying About Cyber Security". Christopher P. Skroupa. *Forbes*. October 27, 2016.

Standing to Sue in Cybersecurity Cases

"Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?". Bradford C. Mank. *Notre Dame Law Review*. 201792 Notre Dame L. Rev 1323 (2017). (PDF)

"Opinion analysis: Case on standing and concrete harm returns to the Ninth Circuit, at least for now". Amy Howe. *SCOTUSblog*. May 16th, 2016.

"Standing in Data Breach Cases: A Review of Recent Trends". Robert D. Fram, Simon J. Frankel and Amanda C. Lynch. *Bloomberg Law*. November 9, 2015.

"Wendy's Data Breach Suit Dismissed Where No Monetary Loss Alleged; Amendment Filed". HHR Advisories & Publications. August 2016.