JUNE 2018

CU*ANSWERS

Key Lessons from Cybersecurity Litigation

CU*ANSWERS
A Credit Union Service Organization

CONTENTS

LEGAL DISCLAIMER

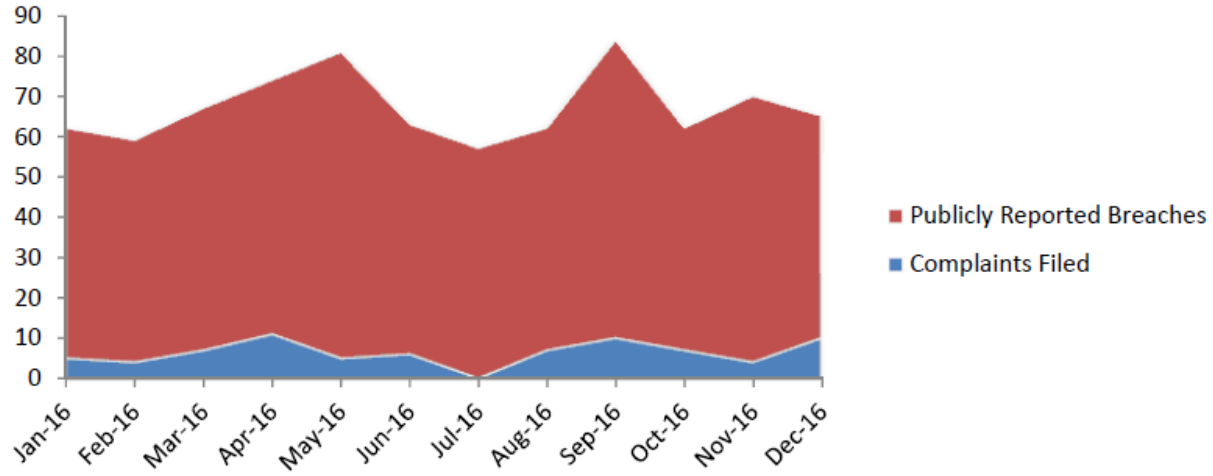
*The information contained in this document does not constitute legal advice. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.*

INTRODUCTION

Lost or stolen records are likely in the billions, possibly tens of billions of records. The sheer volume of records loss implies **data breaches may be inevitable**. Breach statistics and litigation strongly imply breach management is as critical as breach prevention. Every organization has cybersecurity controls, and these controls will at some point fail. What can you do to minimize the damage, the potential liability, the expectations of consumers and stakeholders, and media reaction?

Research from the Bryan Cave Law Firm indicates that the ratio of lawsuits to publicly reported breaches is relatively small. In 2016, there were just 76 class actions filed against companies that suffered data breaches, and 95% of these lawsuits focused on defendant negligence as a legal theory. There is a lot an organization can do to avoid litigation, even where there is fault.

Bryan Cave Data Breach Class Action Litigation Chart



Recent litigation points to three key lessons to help organizations avoid cybersecurity lawsuits: (1) value data properly; (2) have a plan for responding to consumers/public; and (3) know what is and what is not covered by insurance. Any organization can reduce its risk of, or the costs associated with, a cybersecurity breach by learning the key lessons of this litigation.

In re: Anthem Data Breach

Anthem is an American health insurance company. On February 4, 2015, Anthem, Inc. disclosed that criminal hackers had broken into its servers and potentially stolen over 37.5 million records that contained personal medical information from its servers. Twenty days later, Anthem admitted the number was 78.8 million people. The breach spawned lawsuits from all over the country. Ultimately, one hundred and twenty-eight lawsuits were consolidated into one single class action case.

This case was unusual in that it was not settled immediately, and Anthem fought the case vigorously. While this case was very complicated, and this summary is simplified, the main defenses brought out by Anthem included:

- Can't prove consumer harm was due to the Anthem breach;
- Privacy notices are not included in the insurance contract;
- Privacy notices only required Anthem to be compliant
- Compliance with HIPAA
- No monetary damage due to the breach

"Can't prove consumer harm was due to out breach" defense. The court disposed of this defense quickly. The court said "you can't prove it was us" is unacceptable as a defense in the early stages of a case. If the defendant has an alternative theory of the data breach, burden is on the defendant to prove that alternative theory at trial.

Privacy Notice. Anthem tried to say that this Privacy Notice was just a recital of their legal requirements under HIPAA. This defense was rejected because Anthem's contracts Anthem would handle information "subject to all applicable confidentiality requirements" with a cross-reference to the Notice of Privacy Practices.

ANTHEM PRIVACY NOTICE

Anthem Blue Cross and Blue Shield maintains policies that protect the confidentiality of personal information, including Social Security numbers, obtained from its members and associates in the course of its regular business functions. Anthem Blue Cross and Blue Shield is committed to protecting information about its customers and associates, especially the confidential nature of their personal information.

* * *

Anthem Blue Cross and Blue Shield has in place a minimum necessary policy which states that associates may only access, use or disclose Social Security numbers or personal information to complete a specific task and as allowed by law.

Anthem Blue Cross and Blue Shield safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

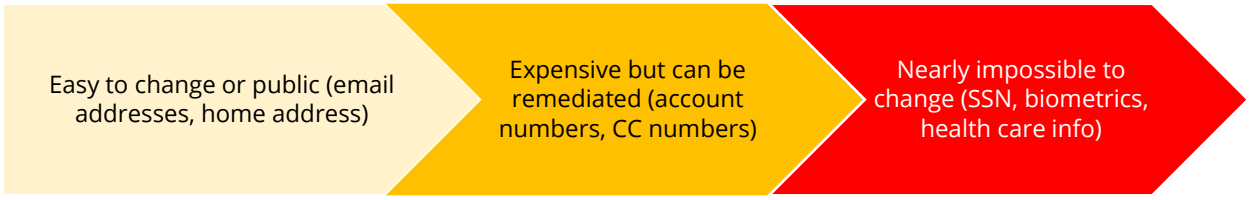
"Benefit of the Bargain" Losses. Anthem's regarding compliance were defeated by a contractual concept known as "Benefit of the Bargain." Plaintiffs paid premiums for health care services that included a promise to have stronger data security measures (see the Privacy Notices). Failure to provide this security entitles plaintiffs to a refund. Put another way, Anthem did not value the data in its custody properly. Anthem was, in fact, compliant with HIPAA, but Anthem promised to protect Social Security and healthcare information over and above its compliance requirements.

The Value of Private Data. Consumers showed their private data was for sale on illicit websites. That mere fact established a "value" for the data. Furthermore, individuals had an interest in the confidentiality and privacy of their information. Therefore, the court found that there was a case for damages. (Note that not all courts agree with this reasoning).

On August 25, 2017, Anthem, an $85 billion company, agreed to settle for $115 million. To date, this is the largest data breach settlement in history.

Lesson 1(a): Some Private Data is Much More Dangerous than Others

Not all private information is created equal. The more valuable the information, and the harder for the individual to change, the more dangerous it is.



The more "radioactive" the data, the greater chance of a lawsuit or other adverse action.

Lesson 1(b): What You Say Can Be Just as Important as What You Do

Organizations should review whether the Privacy Notices/Policies to their consumers accurate, and whether they create a contractual obligation. Consumers may be able to state that the organization created a contractual obligation ("Benefit of the Bargain") or may be able to claim that the organization used Unfair and Deceptive Practices in its communications to the public (e.g. claiming encryption when encryption is not actually applied).

Lewert v, P.F. Chang's China Bistro

On June 9, thousands of compromised cards were put on sale on an illicit website. The common denominator was that every card had been used at a P.F. Chang's restaurant between March and May of 2014. Under intense pressure, P.F. Chang's issued a statement on June 10.

P.F. CHANG'S JUNE 10 STATEMENT

"On Tuesday, June 10, P.F. Chang's learned of a security compromise that involves credit and debit card data reportedly stolen from some of our restaurants. Immediately, ***we initiated an investigation with the United States Secret Service*** *and a team of third-party forensics experts to understand the nature and scope of the incident, and while the investigation is still ongoing, we have concluded that data has been compromised."*

At P.F. Chang's, the safety and security of our guests' payment information is a top priority. Therefore, ***we have moved to a manual credit card imprinting system for all P.F. Chang's China Bistro branded restaurants*** *located in the continental United States.* ***This ensures our guests can still use their credit and debit cards safely in our restaurants as our investigation continues****."*

"Because we are still in the preliminary stages of our investigation, ***we encourage our guests to be vigilant about checking their credit card and bank statements****.* ***Any suspected fraudulent activity should be immediately reported to their card company****."*

This statement told the consumers:

- That the breach must be serious, since the Secret Service was involved (even though P.F. Chang's didn't know the extent of the breach);
- That P.F. Chang's had such little confidence in its technology it was going to a manual card system;
- That it was the responsibility of the consumer to watch the credit reports.

Sure enough, the class action lawsuits began just a few weeks later. Although the total number of restaurants affected may have been small (33 out of 204), the consolidated litigation filed in 2014 is still going on today. (Some 146 filings in the docket)

Lesson 2: Manage the Breach Notifications

Organizations must follow the notification laws of the applicable jurisdiction. However, organizations should be very careful about what the consumers and public are told. In general, avoid sending out a notification until consumers can be told:

- What happened.
- Why it happened.
- What the company will do to prevent it from happening again.
- What the company will do for consumers.

The University of Arkansas completed a study in 2014 measuring consumer responses to compensation offered by a company that suffered a data breach (focusing heavily on Sony and Target). Their findings suggested:

> "Overcompensation" tended to raise customer suspicions. Unilaterally offering extended periods of free credit monitoring for victims of the Target breach led some consumers to believe that the breach was more serious than it actually was.
>
> By contrast, a 10% discount on purchases in the wake of the breach was met with a strongly favorable consumer reaction. This led consumers to the conclusion that Target was truly sorry for what happened and was focused on customer retention.

As with PF Chang's, the "credit monitoring" service and encouraging consumers to be "vigilant" appeared to customers as the company shifting the burden of responsibility from the company to consumers. Target's discount, by contrast, was viewed as the company taking responsibility.

Note, Target still had multiple lawsuits to deal with that did not finally get settled until August of 2017 ($18.5 million). What is important is that Target still maintained customer loyalty during this period.

Have a plan for effectively managing beach response. Understand your responsibilities and consider what you might say to your consumers and the public.

CYBERSECURITY INSURANCE

Cybersecurity policies are still relatively new, and many insurers do pay out, but court cases are trending in favor of the insurer regarding coverage disputes.

P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.

In 2014, Federal Insurance Company ("Federal") sold a "CyberSecurity Policy" to P.F. Chang's marketed as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world." Annual premium was $134,000.

The majority of P.F. Chang's customer transactions were made with credit cards and it contracted with Bank of America Merchant Services ("BAMS") to service all of its credit card transactions. Under that agreement, P.F. Chang's agreed to compensate BAMS for all "fees, fines, penalties, or assessments" imposed on BAMS by credit card associations.

Federal paid more than $1.7 million to P.F. Chang's for covered losses incurred as a result of the June data breach. However, on March 2, 2015, BAMS demanded that P.F. Chang's pay, pursuant to the contract provision, an additional $2 million assessed by the credit card companies as the cost incurred as a result of the data breach. P.F. Chang's submitted the claim to Federal, and this claim was denied. P.F. Chang's sued.

P.F. Chang's argument was that the assessment costs arose out of the data breach (i.e. if there was no data breach there would have been no cost). Federal contested. The essence of the argument was P.F. Chang's took on a *contractual liability* with Bank of America. Contractual liability was excluded under the policy.

Federal Insurance won. The statement that the insurance covered the "full breadth of risks" was not binding. Other cases include Cottage Health, where the insurer tried to rescind coverage because the insured allegedly lied on the application (this went to arbitration); and Spec's Family Partners when the "claim" the insurer was supposed to "defend" did not meet the definitions in the policy.

Lesson 3: Know Your Coverage

Cyber liability insurance is good to have. Financial Institutions and companies just need to understand when coverage will be denied. Will there be coverage for: (1) Contractual obligations; (2) Consumer notification; (3) Regulatory fines and penalties; and (4) Is the insurance application accurate?