
# Cyber Insurance - Read The Fine Print

by Steve Brown

Last year, the FTC and a few dozen law enforcement partners announced a major crackdown on deceptive practices in auto sales, financing and leasing. In one case, the FTC charged that a company deceptively pitched consumers an auto payment program claiming it would save them money--in reality, the fees to enroll in the program averaged $775 on a standard 5Y auto loan. In another publicly disclosed action, the FTC settled claims with three auto dealers whose seemingly favorable sales were canceled out by fine-print disclaimers that did not disclose relevant terms to consumers.

Reading the fine print is one of the cardinal rules of life that many people ignore. Banks, too, can fall into this trap when it comes to cyber insurance protection policies. Financial services firms are being slammed by security incidents a whopping 300x more frequently than businesses in other industries, according to the security vendor Forcepoint, formerly known as Raytheon|Websense. As such, it's no wonder regulators strongly recommend that banks purchase cyber insurance. Many banks have responded to heightened threats by purchasing policies at a considerable cost, but many may not realize the limits of the protection they seek.

Unlike other forms of insurance where coverage is more standardized, there's no standard policy with cyber insurance. Accordingly, banks need to pay special attention to the small print.

Consider the recent case of a Texas manufacturing firm that is suing its cyber insurance provider for refusing to cover a $480k loss following an email scam that impersonated the firm's CEO. Swindlers impersonating the CEO persuaded the company's accountant to wire funds to a bank in China and the insurance carrier reportedly refuses to make the company whole. The issue is reportedly that the scam did not involve the forgery of a financial instrument as required by the policy.

This type of fraud, dubbed business email compromise, is becoming increasingly common. Yet many banks might be shocked to learn that their cyber policies contain an exclusion stating there is no coverage for a "voluntary parting." This exclusion bars coverage when an insured voluntarily parts with property "if induced to do so by any fraudulent scheme, trick, device or false pretense." Some insurers have taken the position that this exclusion applies even in cases where a firm employee was duped into wiring money.

The outcome of the Texas case is certainly something to watch. The case itself underscores the need for banks to delve into the particulars of their coverage, the limits and what protections they are paying for.

There are many other gray areas when it comes to cyber insurance coverage, which is why it so important to understand coverage limits and sub-limits that may exist. Additionally, threats are always evolving and so is the coverage, so what's deemed adequate one year may not be the next. Banks need to review their coverage frequently to ensure they are as protected as possible.

Because there are so many variables with cyber insurance, it's good to seek out a professional who can help you do so. Due to the intricacies involved, brokers who focus on the more standard types of insurance may not be the right person for the job of providing cyber insurance coverage, so think about that too if you decide to do something here.

Cyber insurance is relatively new and banks should proceed with caution because things are changing constantly it seems. Make sure you know what protections you're buying so in the unfortunate event of a cyber-attack, you're covered.

## BANK NEWS

**Cyber Risk**

Research by IT security firm ThreatMetrix finds it detected 21mm cyber attacks against the financial industry in Q4, an increase of 40% over the same period 1Y prior.

**Growth Obstacles**

A survey by Deloitte finds companies say their main obstacles to growth are an uncertain economic outlook (41%), health care costs (34%) and increased regulatory compliance (32%).

**Customer Opportunity**

The population of the US is estimated to be 321.4mm, of which 37% of people live in 5 states: CA (39.1mm), TX (27.5mm), FL (20.3mm), NY (19.8mm) and IL (12.9mm).

**Q4 GDP**

The Commerce Department has revised Q4 GDP from 0.7% originally reported to 1.0%, largely driven by businesses increasing their inventory. Over the past 6 quarters, GDP has been 1.0% (Q4 2015); 2.0% (Q3 2015); 3.9% (Q2 2015); 0.6% (Q1 2015); 2.2% (Q4 2014); and 5.0% (Q3 2014).

**Workforce**

For those tracking demographic trends, baby boomers were the largest part of the labor force from 1995 until 2011. Boomers were then replaced by Gen Xers from 2012 to Q1 2015, who were then replaced by millennials. As of Q1, the workforce was made up of millennials (53.5mm), Gen Xers (52.7mm) and baby boomers (44.6mm).

**Small Biz Digital**

A survey by Wasp Barcode Technologies of small business owners finds: 80% use social media to sell to potential customers.

**Vulnerabilities**

A survey of 300 directors by Deloitte finds crisis areas ranked most vulnerable are: corporate reputation (73%), cyber-crime (70%), rumors (68%), regulatory actions (66%), natural disasters (66%), supply chain issues (66%), organizational malfeasance (64%) and terrorism or man-made disasters (63%). Interestingly, while corporate reputation ranked highest, only 39% said they had a plan to address it.

**Recession Concern**

JPMorgan research finds that when corporate earnings decline for consecutive quarters, a recession follows 81% of the time. This is a concern as corporate profits have been negative since mid last year.