Cyber Liability: Are We Keeping Up?

From Bytes to Bit Coins . . . How Not to Get "Bytten"

Presenters: Ronald Morrison, *Great American Insurance Group*
Shane Riedman, *CNA Insurance*
Matthew J. Smith, *Smith, Rolfes, & Skavdahl*
Daniel Thenell, *The Thenell Law Group*

I. IT IS A SCARY NEW WORLD

This new era of electronic communications has connected the world more than ever. From apps and social media, to online banking and scheduling doctor appointments – today almost everything is done electronically and online. There is even an electronic form of currency called a Bitcoin. However, with these positives there are many negatives. Hackers, "hackactivist," and in some cases, foreign governments, are breaching the network securities of companies worldwide. It is estimate that in 2014, the average cost for a company that had been breached by a cyberattack was $3.5 million.

What does this new era mean for insurance in the future? Are insurance policies changing to adapt to this new era? How will the claims process differ in the age of tweets and texts?

Texts and Tweets, can you stop them as claims and litigation communications?

Text messages and tweets are an efficient way to communicate. However, often times text messages and tweets are made in jest, and may contain loaded words such as "alleged loss," "motive," or "alias." Although some courts allow insurers to claim privilege to documents generated after a questionable claim has been referred to an attorney, in most cases many documents – and communications – generated during an insurer's investigation are not privileged.

Social Media: a wealth of information and a huge risk.

Social media is a wealth of information for investigators and adjusters. Tweets and Facebook posts can assist in identifying and establishing fraudulent claims. Because social media is so prevalent in today's society, it is important for policies and authorizations to obtain information to adapt and include the production of social media

posts during the claims process. In most situations, social media posts are discoverable, however, there may be concerns as to what constitutes an original copy.

What claims are on the horizon?

Cyberattacks and identity theft are on the rise. In this last year, the networks for Sony, Staples, Home Depot, and Target were breached. An astounding 43% of companies worldwide have reported their networks being breached in the past year. The average cost to investigate and respond to these attacks was $3.5 million. In most instances, the information taken from these companies are credit card numbers, and other consumer personal data, which is subsequently sold.

Are Bitcoins covered under an insurance policy?

What is a Bitcoin? A Bitcoin is an electronic form of currency that is not backed by any real asset like a coin or metal. Bitcoins are not regulated by any government, or central bank; instead, Bitcoins are based on a decentralized peer-to-peer transaction system. Bitcoins are exchanged exclusively online. There are no transaction fees, and can be obtained anonymously. Bitcoins are used to purchase items online, but retail stores have slowly begun accepting Bitcoins.

The status of whether Bitcoins are considered currency is still unknown. Bitcoins are often referred to as "digital cash." Unlike typical currency, Bitcoins are mostly unregulated and untaxed. However, a 2013 US District Court, Eastern District of Texas opinion held that a Bitcoin is a security as defined by Federal Securities Laws. *SEC v. Shavers et al*, Case No. 4:13-CV-416 (2013).

Although one district court opinion has defined Bitcoin as a "securities," the issue as to whether a Bitcoin is actual currency will most likely continue to be litigated in the future.

So how does that effect insurance? For example, an insured files a claim for a stolen laptop. The insurance policy provides coverage of $15,000.00 for personal property, and has a $500.00 cash limit. The insured's claim, however, is for the policy limits, because the laptop – worth $2,000.00 – contained $15,000.00 in Bitcoins. What would be the insurer's liability?

Social Media and Defamation.

Although people are not typically sued for defamation, most homeowner's policies provide coverage. With more Facebook posts, tweets, and blog posts, an increase in defamation lawsuits is likely. Most policies do provide exclusions to preclude coverage for defamation claims; however, the insurer may still be required to defend the insured. It is important to note that the duty to defend is much broader than the duty to indemnify. Even though the insurer may not be liable, it may still be required to provide a defense, which could be costly.

Improper use of trademarked or protected data.

How are insurers protecting against improper use of trademarked or protected data?

In *United Westlabs, Inc. v. Greenwich Insurance Company et al.*, 2011 WL 2623932 (Del. Jul. 1, 2011), plaintiff contracted with Seacoast for the SurroundLaw AR billing system ("SLAR"). Shortly thereafter, plaintiff notified Seacoast of problems with SLAR, and terminated Seacoast's access to its VPN. In early 2007, plaintiff and Seacoast commenced arbitration, but later agreed to dismiss their claims in an attempt to reconcile their agreement. In September, 2008, plaintiff's policy with defendant Greenwich commenced. Plaintiff did not disclose the issues involving Seacoast in its application for insurance.

In December, 2008, attempts at reconciliation between plaintiff and Seacoast failed, and again, plaintiff denied Seacoast access to its VPN. Plaintiff brought claims against Seacoast, and Seacoast counterclaimed, alleging that plaintiff had committed copyright infringement. Plaintiff tendered the defense of the counterclaim to defendant Greenwich, which later denied coverage. Plaintiff filed suit against defendant Greenwich alleging it was obligated to defend it against Seacoast's claim of copyright infringement. Defendant Greenwich filed its motion for summary judgment on the grounds that plaintiff's claim fell outside of the applicable policy periods. Defendant Greenwich's motion further alleged that there was no duty to defend because the policy included a "Intellectual Property Exclusion." The policy stated in pertinent part that:

> The Insured shall not recover for any claim "based upon, arising out of, directly or indirectly resulting from, in consequence of, or in any way involving any actual or alleged:
>
> (1) infringement of any patent , copyright or trademark; or
> (2) unauthorized taking or use of any trade name, trade dress, trade secret, service mark, service name, title, slogan, proprietary process, material or information, other material or information in violation of any right under any patent, copyright or trademark registration or license, or any other intellectual property.

The Court granted defendant Greenwich's motion, holding that the counterclaim made against plaintiff existed before the applicable policy period, and thus, did not decide whether the "Intellectual Property Exclusion" was applicable. However, the exclusionary language in the policy appears sufficiently to protect the insurer against liability.

Every claim has the potential to go viral.

From blogs to news outlets, every claim has the potential to go viral. It is important to be wary for the potential of negative claims to be the hot 24 hour news cycle.

II. WE ARE WINNING THE INITIAL BATTLES IN COURT

Discovery of electronic communications and social media

The Federal Rules of Civil Procedure (FRCP) saw this electronic era coming, and specifically include the production of electronically stored information. FRCP 26 states in pertinent party that a party must provide the other parties "a copy – or a description by category and location – of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment." FRCP 26(a)(1)(ii). A party may request production of any designated documents or *electronically stored information*. FRCP 34(a)(1)(A). Electronically store information must be produced as they are kept in the usual course of business, in a form or forms in which it is ordinarily maintained or in a reasonably usable form. FRCP 34(b)(E).

The term "electronically store information" is broad enough to cover all types of electronic based information, and is flexible to adapt to future changes. Given the FRCP's liberal use of the term, it is important to request electronic communications during the course of discovery.

Court sanctions for spoliation of evidence

Evidence spoliation occurs when an entity, or individual, does not preserve evidence relevant to a pending litigation. "Prudent parties anticipate litigation, and begin preparation prior to the … time suit is formally commenced." *Lamar Advertising of S.D., Inc. v. Kay*, 267 F.R.D 568 (S.D. 2010) citing *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 604 (8th Cir. 1977).

A massive amount of information can be stored electronically and online, and thus, it is important that once litigation appears likely it is important that a litigation hold is put on all documents that may be relevant. Courts have significant latitude in imposing sanctions for spoliation of evidence. The Court's authority is derived from the Rules of Civil Procedure, and includes imposing fines and attorney fees.

For example, in *Lester v. Allied Concrete Co.*, 2011 WL 9688369, the plaintiff sent defendant's attorney a message via Facebook. This allowed defendant's attorney access to plaintiff's Facebook page, and requested its production. Plaintiff was instructed by his attorney to "clean up" his Facebook page of any negative photographs and posts. Plaintiff then deleted 16 photographs from his Facebook page. The Circuit Court of Virginia imposed attorney fees and sanctions against plaintiff and his attorney for the deletion of the Facebook photographs.

Computer virus claims and fraudulent wire transfer losses

In *State Bank of Bellingham v. Bancinsure, Inc.* No. 13-cv-0900, 2014 WL 4829184 (D. Minn. Sep. 29, 2014), the loss stemmed from a fraudulent wire transfer. In the course of defendant's investigation, it was determined that plaintiff's employee had used the company computer for personal use, downloaded a virus through spam email, and failed to enable and update antivirus software. Defendant moved for summary judgment, arguing that coverage was excluded due to the loss being caused by plaintiff's employee.

The Court disagreed, stating that when there are multiple causes for an insured's loss, one of which is covered, and the other excluded, "Minnesota's concurrent causation doctrine provides that the availability of coverage or the applicability of the exclusion depends on which peril was the "'overriding cause'" of the loss." *Bancinsure* * 19 citing *Friedberg v. Chubb & Son, Inc.*, 691 F.3d 948, 952 (8th Cir.2012). Although plaintiff's employee did violate numerous policies and practices of the plaintiff, it was the criminal activity that caused the loss. *Bancinsure* *21. In other words, without the "fraudster's actions, there would have been no loss" even with the employee's conduct. *Bancinsure* *21.

But compare *Bancinsure* with *Universal City Studios Credit Union v. Cumis Ins. Soc., Inc.*, 208 Cal.App.4th 730 (2012). In *Cumis*, the plaintiff, a credit union, processed a fraudulent wire transfer, and sought to recover its loss under a bond issued by defendant. Prior to the fraudulent wire transfer, the defendant modified the "Funds Transfer Coverage." The modification required either a callback verification security procedure, or a signed written agreement with the member agreeing to another type of security procedure, for all transfer requests received through fax, telephone or email.

In 2008, the plaintiff received a request for a wire transfer via facsimile. The plaintiff, however, did not follow the callback verification procedure under the modified "Funds Transfer Coverage" language. Moreover, the bond's coverage for Forgery included an exclusion for any loss directly or indirectly from fraudulent instruction through email, facsimile or telephonic means except as may be covered under the "Funds Transfer Coverage."

III. SLOW TO CHANGE BUT CHANGE WE MUST

Many insurance policies contain language that is outdated in this new era of electronic communications. Policy language must be updated to include new definitions to limit exposure and losses. Moreover, with the increase in cyberattacks and identity theft, policies must be modified to ensure that if coverage is available, all reasonable steps are taken to prevent the fraudulent activity.