PREPARING FOR INTERNET CLAIMS: SECRETS FOR SUCCESSFUL HANDLING OF E-CLAIMS

The rapid growth of e-commerce and internet use in recent years has inevitably brought with it a rising volume of new claims. In important respects, internet claims are different from claims traditionally presented under property and casualty policies and demand new approaches by claim professionals. Knowing the differences is critical for the successful handling of internet claims.

Reactive claims handling simply will not work with this new breed of claims. In the world of cyber claims, the evidence trail is too transitory and the damages accumulate far too quickly for the traditional adjusting process. The key to success in handling e-commerce claims is preparation. Speed and technological expertise are essential for diagnosing internet events, stemming ongoing losses and identifying cyber culprits. The way to secure those essential resources is to assemble a technological/legal response team before first notice of a claim.

In this article, we introduce the method for successful handling of internet claims in three steps. In Section I, we provide a description of the most common internet events that will be presented in insurance claims. In Section II, we examine what makes these claims different from claims encountered in the past and why new rules of engagement apply. In Section III, we more fully describe the method for successfully handling e-commerce claims. This analysis is offered both to demystify cyber claims and to provide an initial plan to guide you in adjusting these claims.

I. INTERNET EVENTS THAT PRODUCE CLAIMS – WHAT TO EXPECT.

The universe of potential internet claims is limited only by the ingenuity of the hackers, vandals and cyber thieves who roam the web. In other words, the variety of cyber claims you may see is virtually unlimited. Describing potential internet claims can be nothing more than a snapshot of an electronic rapids, because the incessant change in technology and methodology renders any description out of date as soon as it is written. That being said, the current generation of internet events giving rise to claims can be loosely divided into four groups.

Availability Attacks.

One type of internet event that has attracted a lot attention in the past year is the *availability attack*. Availability attacks cause losses by preventing authorized users from accessing internet resources. These attacks may be malicious, but they can also be caused unintentionally or carelessly. Some are extremely complex, while others rely upon very simple methodologies.

Currently, we encounter two basic types of availability attacks: *blocking attacks* and *flooding attacks*. A blocking attack stops authorized users from accessing a resource by physically or electronically destroying a route to the resource. Physical denial of service is the most common non-malicious blocking attack. Communications lines may fail, applications software and server hardware may crash, or systems may inadvertently be reconfigured in a way that prevents access. Malicious blocking attacks may occur when an attacker accesses a system to destroy or delete critical files, invalidate accounts or change access control protocols.

A flooding attack stops authorized users from accessing a resource by overloading the system with a large number of directed inputs. A flooding denial of service attack typically exploits a flaw in the design or implementation of a network protocol, operating system or commonly used application. Common examples of flooding attacks are the *SYN flood*, which bombards a site with

SYN packets used to open a connection. With an *e-mail bomb*, the attacker sends a large number of messages in attempts to overrun a system's or an individual user's e-mail storage. A *smurf attack* uses a PING packet in broadcast mode with the forged return address of the intended victim. The PING is broadcast to a large number of systems, all of which respond by sending PING packets to the intended victim.

A *distributed denial of service attack* multiplies the effect of an ordinary denial of service attack by launching it simultaneously from multiple sites. This is accomplished by the attacker gaining access to a number of sites in advance and planting code in each to launch the attack at a preset time or on a signal. Using such remote sites provides a measure of invisibility to the attacker, which makes distributed denial of service attacks difficult to trace and prevent.

Integrity Attacks.

Integrity attacks are attacks that change or destroy source content. With an integrity attack, authorized users can gain access, but what they find when they get there is not what is supposed to be there. Integrity attacks can be, and often are, non-malicious in origin, as many unintentional causes may corrupt or modify data. However, malicious integrity attacks are becoming both more common and destructive.

Malicious code comes in a variety of forms. Best known is the virus. A *virus* is a piece of code that includes a means by which it spreads itself to other users. A recent form of virus is the *macro virus*, which is implicated in macro commands in standard commercial packages such as Microsoft Word or Excel. These macros are attached to documents that people exchange, which become their method of propagation.

A *Trojan horse* is another variety of malicious code with a hidden, harmful function. Trojan horses can be inadvertently downloaded from a web server in the guise of Java applets, Active-X

controls and other add-ins that support the processing of data. The user is typically unaware that code has been received, and, even if aware, effectively unable to determine that the code does only what it is supposed to do. A Trojan horse is often combined with a virus, giving it both malicious behavior and the ability to propagate.

A *forgery* or *counterfeit attack* presents data with a false representation that it has come from another. On the internet it is reasonably easy to provide a false source address for a communication, which facilitates message forgery. An attacker can also hijack a session by intercepting a communication session and continuing it in the name of (and with the privilege of) the victim.

A *stack overflow attack* is one in which the attacker intentionally supplies a very large amount of input (for example, 2,000 characters in a name field), in order to exceed the space allocated for an input and spill over into adjacent data or code areas, either corrupting other values or inserting new commands to be executed.

Confidentiality Attacks.

Confidentiality attacks are attacks that expose confidential data to the view of unauthorized readers. Unlike an integrity attack, a confidentiality attack does not alter the content of a source, but only affects the security level and dissemination of the source. However, confidentiality attacks may be used as a first step in availability or integrity attacks, as where the attacker obtains confidential passwords to gain unauthorized access.

A confidentiality attack may defeat incryptions of passwords or simply engage in password guessing. Wire tapping may be used to intercept internet traffic. Or, a packet sniffer may be used to copy each packet on a network and filter out unwanted traffic. Confidentiality attacks may take the form of commercial appropriation of confidential information. Most involve intrusions and

disclosure of private facts that are not commercially motivated, but are undertaken solely for the amusement of the invader.

Property Rights Infringement Claims.

Trademark, *copyright* and *patent infringements* that occur on the internet enjoy no special privilege under the laws. Due to the shear volume of new material, the novelty of the medium and the general disregard of legal niceties by cyberworld visitors, intellectual property claims find a fertile environment on the internet.

As the name suggests, copyright law prohibits the copying of certain protected materials, which may include computer programs, literary works, sound recordings and graphics. Copying may occur whenever an item is printed, cut and pasted, or downloaded. Copying is an essential function of modern computing, and it is easier than ever before on the internet. Intellectual property lawyers are only beginning to warm up to the possibilities here.

Trademark laws seek to prevent confusion between similar trademarks and dilution of a mark's capacity to identify and distinguish goods and services. At least three new types of trademark infringement claims have arisen from the internet. The first type is the *domain name dispute*. A company's domain name is not only its unique identification marker but also its electronic address. A domain name that is confusingly similar to another may violate traditional trademark laws, as well as new anti-cybersquatting legislation.

The second type of unique internet trademark claim involves *meta-tag disputes*. A meta-tag is a key search term imbedded in a web page by its designer to attract traffic to the site. When a term is keyed into a search engine, the search will call up all pages that contain the term in their meta-tags, whether or not the term actually appears on the page. It is technologically possible for a party to use another party's trademark as a meta-tag for its own site, for the purpose of bringing

traffic to the site as a result of the misdirection. The unauthorized use of trademarks in meta-tags is as actionable as the unauthorized use of trademarks in readily readable form on a web page.

The third new type of internet trademark dispute involves *linking* and *framing*. By linking, a page designer makes it possible for a web user to click on an icon and transfer immediately to another web site. Framing is a variation in which the second site is made to appear as part of the first. *Deep links* can be used to transfer a user to a second site, bypassing the home page and other identifiers of the second site. The effect on the user is a fairly seamless transition from the first site to the second, making the second to appear as part of the first site.

New forms of patent infringement are also developing with the internet. Internet methods of doing business are patentable, and the number of internet-related patents is quickly growing. Internet patent infringement suits have already been filed, and more will undoubtedly follow.

II. THE UNIQUE CHALLENGE OF INTERNET CLAIMS – WHAT MAKES THEM DIFFERENT.

It is a mistake to believe that internet claims can be successfully handled by the same procedures and protocols used in the past. In order to accomplish anything useful in the handling of an internet claim, it is necessary to act very quickly and with a high degree of technological sophistication. Claims handling in this environment must be a 7/24 proposition. Thirty-day diary dates have little place here. The first 48 hours are critical, and the most important work on the file should be completed within the first 7-14 days.

Everything happens quickly on the internet, and events that do mischief happen the quickest. There are at least three reasons why. First, internet events are capable of traveling around the globe, and to every point on the globe, at the speed of an electrical impulse. Second, all stations in the internet are linked by myriad pathways, so that any isolated event can be transmitted automatically

and almost simultaneously to stations everywhere. Third, because the internet is so vast and complex a network, finding and stopping unwanted causes is extremely difficult.

On the internet, damage occurs at the speed of an electronic impulse and propagates geometrically. In availability attacks, lost profits escalate second by second as would-be visitors and purchasers are denied access. In integrity attacks, the damage may be ongoing and progressive, not only corrupting more data with every tick of the clock, but also further complicating efforts to analyze causation and efforts to remediate. In confidentiality attacks, loss typically grows as the sensitive information is revealed to each new viewer or put into use by unauthorized persons. Property rights infringements also accumulate damages as the infringements are increasingly exposed to other viewers and put to unauthorized uses. Each minute and hour that a harmful event remains unresolved can mean substantial additional damages.

A new timetable must apply to the handling of internet claims. Not only because the damages progress at a startling rate, but also because the evidentiary trail is extremely transitory and fragile. The trail of the cyberworld tortfeasor are footprints in the dust, clearly identifiable but for a few moments and then lost to time. With these claims, there is little time for pondering coverage questions or thinking about who to call to investigate and respond to the loss. What is needed is an immediate diagnosis of what has happened (or what is still happening) and implementation of a plan to bring the event to a halt.

Keep in mind that with internet events, unlike traditional loss scenarios, it usually is not immediately clear what is happening, much less what is causing the loss. When vehicles collide or the proverbial surgical sponge is left inside a patient it is easy to identify the occurrence, but a darkened computer screen can mean a lot of different things. Without immediate technological assistance, you will not know what has happened behind the darkened screen, whether the cause is

malicious or accidental, whether the loss sequence is completed or ongoing, and you will have no idea about what to do about the problem. The longer it takes a claims handler to accurately analyze these issues, the more the damages will have a chance to accrue.

The principal objective in handling internet claims is to stop the unwanted event. Because the evidence disappears so quickly and the damages grow so rapidly, everything else must take a back seat. If you have an uncontrolled, ongoing loss in progress, there is not much point in undertaking any of the other efforts associated with claims handling. Until you assign investigators to assess the event, there is no possible way you can know what is really happening. And until you begin to diagnose the event, critical evidence will be lost. Without either evidence or a cap on the accruing damages, the result can not be good, no matter what else you might normally do on a file.

Chasing the wrongdoer, when a wrongdoer is involved, is of secondary importance. The wrongdoers of the cyberworld are elusive, so they can be difficult to trace. They literally can be at work anywhere in the world, so even if you can find them, you may have trouble doing anything to subdue them. They usually also lack assets to compensate for the losses they cause, so the hope of subrogation is illusory in these claims.

You will probably see more first party claims arising from internet torts than third party claims, simply because the victims of the cyber world so outnumber the wrongdoers. One malicious hacker is capable of causing injury to thousands or millions of others on the internet. The extent of third party claims will depend largely on coverage questions that have yet to be judicially determined under the old policies and the new e-commerce policies. Presumably, intentional acts will not be covered under any of the policies, but carriers may find themselves having to provide a defense even in such cases. Early notice in all claims will increase the carrier's potential for effectively controlling and responding to the loss.

III. WHAT TO DO – PREPARING FOR E-COMMERCE CLAIMS.

When internet claims strike, there is little time to waste. You need a plan firmly in mind and a response team ready to take your call. Finding the right personnel takes time, which you can ill-afford once you have received notice of a claim.

The team you need to successfully handle internet claims consists of three vital elements: (1) an internet investigator/analyst; (2) an attorney; and (3) an internet expert. Using the same investigators, lawyers and experts who you use for other property and casualty claims will probably be a big mistake, as these claims do not allow time for on-the-job education. When assembling your team, you need professionals with experience and demonstrated competence with similar claims.

The Internet Investigator/Analyst.

The duties of the internet investigator/analyst are among the most critical and must be undertaken immediately upon notice of a claim. The first task of the investigator/analyst is to ascertain what has happened (or is continuing to happen). This is more difficult than it may seem. Often, when a claim comes in, all you know is that some data has been lost or a system has crashed. A first report usually identifies only certain symptoms of the underlying problem, and you have little indication of the broader picture. Before anything else can be done, it is essential for the investigator/analyst to identify the nature of the attack and whether it has been completed or is still in progress. Only then can the urgency and seriousness of the claim be ascertained. The investigator/analyst is capable of peering beyond what is visible to most to diagnose the complained of condition.

The second task for the investigator/analyst is to assess causation: what caused, or is causing, the loss? Is it a systems defect, a negligent error, or a malicious attack? Are you dealing

with a narrowly focused attack or a web-wide assault? Identification of the cause gives helpful insight into the potential extent of the damage. It also provides important clues for putting solutions into effect.

The third task for the investigator/analyst is to stop the loss and remediate the harm. Even when the problem and its source have been identified, those facts do not immediately provide the answer of how to freeze the unwanted event. This task is not finished until all data and facts are restored, and the victim is back in business.

The Role of the Attorney in an Internet Claim.

The lawyer's role in internet claims should be different than with most claims. The lawyer's timetable in these cases, like that of the investigator/analyst, is very short. The primary task of the attorney is not to seekn damages in these cases, but to help stop the loss and restore the victim to operation. In the early investigation of the claim, the lawyer should assist in obtaining access and evidence where legal process is required to provide the investigator/analyst with what he needs. The attorney should also be on hand to address delicate privacy issues which may arise during the course of the investigation. Further, the lawyer and the investigator/analyst should work together to identify the technological and legal causes of the damage in question.

Once the cause is identified, the attorney's role is essential in providing legal means to stop the loss, by obtaining emergency injunctive relief in court. Obtaining judicial relief in these cases is often complex, as the identification of a wrongdoer operating on the internet involves novel and difficult jurisdictional issues. Working closely together, the lawyer and the investigator/analyst can implement both technological and legal devices to halt further damage.

After all urgent needs have been met, the attorney may then return to her more traditional role of assessing the potential for economic recoveries.

The Expert.

The expert on the team should assist the investigator/analyst and the lawyer in the earliest stages of the claim. The expert can assist the investigator/analyst by serving as a consultant and by providing second opinions when decisions must be made during the early course of the investigation. The expert can assist the lawyer by providing the testimony necessary for the lawyer to obtain the discovery and emergency relief sought in such cases. Later, if damages are sought, the expert can also testify in support of that claim.

Although the necessary qualifications of these professionals are not widely held, the identification of an internet claim response team can be less daunting than it may seem. If you find an attorney who works on such claims, she will undoubtedly have investigators/analysts and experts to recommend. Or, if you find an appropriate investigator/analyst or expert, chances are very good that those professionals will also be able to recommend other team members. Due to the worldwide nature of the internet, you may not need teams in every jurisdiction, only teams with sufficient resources to appear when and where you need them.

CONCLUSION

Success in handling internet claims depends 80 percent upon your retention of a ready and qualified response team, and 20 percent upon quickly beginning the investigation. Preparation is everything. Once you and your response team identify the unwanted internet event and stop it, the claim becomes (almost) routine. At that point, you can follow the normal protocols and analyses, but until the situation is stabilized, the outcome can only be bad.

By assembling your response team in advance, you can assure that when internet claims are reported, you will be able to make meaningful inroads toward resolving the matter without delay. By doing this now, you will save days or weeks in the critical early period of a claim.