October 19, 2001

Recovery Opportunities in Computer Virus, Hacking and Other Ecommerce Claims
By: Zacarias R. Chacon, Esq., Cozen O’Connor

I. Coverage – The Prerequisite for Subrogation

In the Federal District Court decision rendered in Arizona in American Guarantee v. Ingram Micro, 2000 WL 726789 (D.Ariz.2000), the court found coverage under a first party policy for a network system’s “loss of functionality” resulting from data loss. The court based its finding of coverage on the following reasoning:

At a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram’s broader definition of ‘physical damage.’ The Court finds that ‘physical damage’ is not restricted to physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.

Some companies have already developed products specifically aimed at providing coverage for WebPerils. The products are expressly designed to protect insureds against losses intrinsic to a web presence, including:

- Losses to data resulting from virus introduction, hacking, loss of power, denial of service attacks and other WebPerils;
- Resulting business income losses

Thus, insurers increasingly will be faced with claims for losses peculiar to ecommerce. The next consideration by claims management will be whether claim payments can be recovered from responsible third parties. The purpose of this paper is to address recovery opportunities for losses resulting from WebPerils.

*Affiliated with the Law Offices of J. Goldberg, C. Stuart, III, & D. Grossman.*
II. Web Peril Terminology

*Virus* – *Viruses* are computer programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but is not designed to spread itself from that computer to other computers.

*Worm* – A *computer worm* is a program that is designed to copy itself from one computer to another over a network (e.g. by using e-mail). The worm spreads itself to many computers over a network, without direct human assistance. This means that computer worms spread much more rapidly than computer viruses.

*Trojan Horse* – A *Trojan Horse* is a computer program that masquerades as a helpful program, but turns out to be malicious code. Trojan Horses do not replicate.

*Hack* – A *Hack* is an unauthorized use or entry into a computer or network system.

*Cracker* – A *hacker* who gains unauthorized entry into a computer or network system with the intention of destroying, damaging or changing the system for personal gain, revenge or a thrill.

*Payload* – The *Payload* is the malicious activity that the virus performs. Not all viruses have payloads.

*Denial of Service Attack* - A *denial of service* (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system.

III. The Potential for Loss

The potential for loss from WebPerils is *significant*. According to the Computer Security Institute’s “2000 Computer Crime and Security Survey” of March 2000, 90% of respondents detected computer security breaches in the previous 12 months. Examples of security breaches included:

- Computer viruses
- Laptop theft
- Employee “net abuse”
- Theft of proprietary information
- Financial fraud
- System penetration from outsiders
- Denial of service attacks
- Sabotage of data or networks
Losses from 273 respondents (40% of those surveyed) totaled $265,589,940.

Moreover, Lloyds of London estimated that losses attributable to the “Love Bug” at $10 billion. This figure includes lost business, the cost of eliminating the virus from computer systems and the cost of repairing, to the extent possible, damaged computer files.

IV. Potentially responsible third parties

a. Telephone companies and other utilities

A telephone company or electric company may be legally liable when an interruption in telephonic or electric service causes loss of data or lack of functionality. Indeed this was the scenario in American Guaranty v. Ingram Micro where the loss was precipitated by a loss of electrical power to the insured’s location. Claims may be made for loss of data or loss of systems functionality where electrical power to an insured location is interrupted. In addition, loss of dial-up or DSL access to the internet, because of telephone service interruptions, may result in serious business income losses.

b. Internet Service Providers

Internet Service Providers (ISPs) may be responsible for interruptions in service and denial of service attacks. For example:

- Company A loses business because the ISP does not adequately protect against a denial of service attack.
- Company B has a commercial web site that goes down due to a malicious hack on the ISP that could have been prevented with proper security measures.

c. Firewall manufacturers and software providers also may be responsible for losses resulting from hacker and virus attacks. For example:

- A failure of firewall software may allow an unauthorized user to access network resources and steal or cause damage to information stored on the network in electronic form.
- Anti-virus software may fail to detect a virus that is part of a file downloaded off the Internet.
- A security flaw in email software may permit receipt and execution of email worms like the “I love you” worm;
- A security hole in browser software may permit unauthorized access to network resources.
d. Other Companies Connected to the Internet

Companies with a presence on the web also may be responsible for losses resulting from hacker and virus attacks. For example:

- After Company A is infected with an email worm, outgoing email triggered by that worm infects Company B. Appropriate security measures by Company A may have prevented the infection of Company B.

- Employees of Company A conduct a destructive or larcenous hack on Company B.

- Employees of Company A deliberately send an email attachment worm to Company B.

e. Installers and Design consultants

- A system installer may neglect to properly configure firewall or virus protection software

- A network design consultant may fail to recommend adequate firewall or virus protection software

V. Recovery for Losses Resulting from WebPerils

a. Actions against Utilities and Telephone Companies

Liability for losses caused by service interruptions may be governed by tariffs approved by the commission or board charged by the state with responsibility for regulating the industry. Examples of tariffs governing the liabilities of utilities may be found in Premier Parks v. Baltimore Gas & Electric Co., 37 F.Supp.2d 732 (D.Md. 1999) and Houston Lighting & Power Co. v. Auchan USA, Inc., 995 S.W.2d 668 (Tx. 1999). These tariff provisions purported to limit the utility’s liability.

Although existing tariffs may have the effect of making recovery against utilities more difficult, there are circumstances under which those tariffs will not be enforced because they are unconscionable, constitute adhesion contracts or cause a failure of the essential purpose of the contract.

b. Actions against Internet Service Providers

An ISP’s relationship with its customers may be governed by a contract with a limitation of liability. An analogy can be made to the theories under which tariffs have been held inapplicable or unenforceable.

c. Actions against software manufacturers, network design consultants and installers

Many software licenses, network design agreements and installation or consulting agreements contain limitations of liability. An easy analogy can be made to similar limitations of liability and
exculpatory clauses in fire and burglar alarm contracts. These limitations generally will not be upheld in the face of unconscionability, ambiguity and gross negligence.

\[ d. \quad Actions \text{ Against Other Companies} \]

Those examples of deliberate misconduct against one company by an employee of another company in the form of a destructive or larcenous hack or deliberate virus infection may, depending on the circumstances, impose vicarious liability on the employer of the malfeasants.

Moreover, the failure of a company to adopt safeguards against the accidental spread of viruses and worms may result in their liability for loss and damage caused by such malicious software that passes through but does not originate in their system.

VI. Conclusion

Although the technology issues that give rise to the types of losses discussed here are relatively arcane, many of the legal issues raised have been addressed in other contexts. While it may be difficult to make general statements about the overall feasibility of subrogation recovery for losses resulting from WebPerils, it is important to keep recovery considerations in mind when dealing with these novel types of losses.

For additional information, please contact:

Richard C. Glazer, Esquire  
Chair, Subrogation Department  
Cozen O’Connor  
1900 Market Street  
Philadelphia, PA 19103-3508  
Telephone: (215) 665-2000  
e-mail: rglazer@cozen.com

Elliott R. Feldman, Esquire  
Director, National Subrogation Programs  
Cozen O’Connor  
1900 Market Street  
Philadelphia, PA 19103-3508  
Telephone: (215) 665-2000  
e-mail: efeldman@cozen.com

Vincent R. McGuinness, Esquire  
Cozen O’Connor  
1900 Market Street  
Philadelphia, PA 19103-3508  
Telephone: (215) 665-2000  
e-mail: vmcguinness@cozen.com

©Cozen and O’Connor. All Rights Reserved.