techLAW

the link between law and dot.commerce

A Publication of

FARRELL FRITZ, PC

Trusted advisors to Long Island's leaders

Issue 2, Volume 1
Winter 2001

Insurance Coverage For Computer-Related Losses

By Eric W. Penzer
epenzer@farrellfritz.com

The headlines in recent months reveal the increasing frequency with which companies are being victimized by computer-related crime. What's more, the list of victims includes some of the best known technology companies, including Microsoft and AT&T. The lesson is clear: if Microsoft, with all of its technological resources and advanced security measures, can fall prey to cybercrime, so can any other company.

The stakes are high. A cybercriminal may infiltrate a company's computer network in the hopes of accessing intellectual property, such as customer information, source codes, trade secrets, and patents. In the hands of a competitor, such information can be damaging to its rightful owner. It is also possible that a company's business will be crippled by viruses sent to the general population. Such viruses, when unknowingly downloaded by an employee, have the potential to eradicate data from computer systems, crash e-mail systems, intercept passwords, and otherwise interrupt business. It is estimated that the Love Bug virus that circulated in May 2000 caused billions of dollars in damage in less than one day.

For several years now, insurance policyholders have sought coverage for computer-related losses under "traditional" business insurance policies. Although these policies arguably were not designed to address computer-related losses, it is possible that they do provide coverage for some computer-related losses. This determination will, of course, turn on an analysis of the insurance policy itself. Among those areas that must be analyzed are the definitions contained in the policy, the scope of coverage, as well as the policy exclusions.

The definitions contained in the policy may restrict coverage to physical damage or tangible property. Other definitions may be broad enough to include some computer-related losses. For example, some traditional policies cover losses resulting from "direct physical loss of or damage to covered property." Others cover various types of losses resulting from business interruption. Some policies may even contain

continued on page 5

Workplace Privacy Issue Gets Attention

During the past three months, Farrell Fritz Partners Kathleen Tomlinson and James Wicks have spoken about the growing issue of workplace privacy twice: to corporate and non-profit executives at the C.W. Post Business Institute on November 8, 2000 and to a group of corporate counsel at the Long Island chapter of the American Corporate Counsel Association on January 17, 2001. With a number of new bills pending and enacted, this merging of the areas of technology and employment law is getting more complex and difficult for human resource and other corporate executives to manage. How are the privacy expectations of employees conflicting with the needs of

continued on page 4

The "Long Arm" of the Law

By Michael J. Healy
mhealy@farrellfritz.com

The case law is now crystalizing on an issue, germane to all who conduct business through a Web site, that applies an age-old legal principle in the context of today's e-commerce world — the ability to be sued in an out-of-state court based on Internet Web site activity.

The issue offers more than passing technical interest to legal scholars. It provides real, practical consequences to all who use Web sites to conduct business. The question involves what is known as "long-arm personal jurisdiction," and centers on the power of a court to hear and determine a case against an out-of-state defendant who uses

continued on page 5

Inside This Issue

FARRELL FRITZ, PC
EAB Plaza
Uniondale, NY 11556-0120
(516) 227-0700
www.farrellfritz.com

I Know What You Bought Last Summer:
The Collection of Consumer Information on the Internet

By Joseph M. Gitto
jgitto@farrellfritz.com

Browsing the "Jazz" section of a popular online music retailer, you come across a limited edition Miles Davis CD you have wanted. So, you click on the album and it is sent to your "virtual shopping cart" at which point you choose to proceed to the "checkout." A few days later, the CD is waiting on your doorstep. Interestingly, the next time you click on that same site, you notice that most of the advertisement banners on the page are for jazz-related music and books. Perhaps even more interesting is the sudden surge of catalogs and advertisements for jazz and music-related items being delivered to your home. It seems that the whole retail world now knows that you like listening to jazz, and is beckoning you to buy more. What exactly happened when you bought that CD?

How Information is Collected

In the past, due to a general lack of consumer protection laws in the United States, it was common for retailers, especially mail-order and catalog-only retailers, to exchange consumer information with one another. This information market was made more viable, accessible and lucrative, with the increased popularity of the Internet and the ability of consumers to make purchases online. It soon became standard practice to key advertising and other commercial solicitations to the products purchased online by individual consumers. Thus, when a consumer purchases an item from an online retailer, a list may be compiled consisting of that consumer's name, address, items purchased, quantity purchased, payment method, etc. This information may then be sold to other retailers who can then cater their advertising to that consumer's particular tastes. Thus, these data collection methods make for more effective, cost-efficient advertising . . . and decreased privacy.

A Public Outcry

With the development of keyed advertising, there came a "consumer backlash." Consumers demanded that they be informed when their personal information is given to other retailers as a result of making an online purchase. In response to these concerns, the legislature proposed the Online Privacy Protection Act of 1999 ("OPPA"), which set out to impose strict limitations on the methods by which a retailer may use the information gleaned from a consumer's online purchases. Some of the key provisions of the statute concerned full disclosure by the retailer with respect to the type of personal information that is collected, what personal information would be shared with others and the method by which a consumer could consent to or limit the information shared.

Despite Act's Demise, Debate Continues

Due to constant pressure by Internet companies, the OPPA never made it out of committee at the close of the 106th Congress and, thus, must be reintroduced. Despite the demise of the OPPA, it is certainly not the end of the debate over online consumer privacy. Technology industry lobbyists have stated that one of the biggest congressional battles to be fought in the new congress will be over online privacy. One of the most controversial issues is the application of either "opt-in" or "opt-out" information gathering. Using an "opt-out" method of information gathering allows consumers to inform the retailer that they do not want any personal information collected. "Opt-in" forces the retailer to get consumer permission before undertaking any information gathering activities.

> ***This information market was made more viable, accessible and lucrative, with the increased popularity of the Internet and the ability of consumers to make purchases online.***

Federal Privacy Legislation May Have Unexpected Support

While it is likely that any proposed legislation will be opposed by technology lobbying groups, recently there has been a surprising policy reversal on the part of one of the largest and oldest high-tech trade organizations. The American Electronics Association, which has become concerned by the vast differences in state imposed online privacy regulations, has pledged its support for federal privacy legislation. The federal legislation would supersede state laws dealing with online privacy. Such a change in policy may help online privacy legislation go forward in the future.

As the number of online purchases increases exponentially with each passing year, more and more consumers will be wondering how many other people know where their tastes lie regarding such things as books, clothing, food, and music. It seems it is only a matter of time before online privacy legislation is passed. Only the question remains whether the legislation will go far enough to safeguard against the concerns of consumers.

...And you thought you were just buying a CD?

Joseph M. Gitto is an associate in the Commercial Litigation Department.

Privacy for Financial Institutions' Customers:
Complying with the Gramm-Leach Privacy Regulations, Electronically

By Christopher P. Daly
cdaly@farrellfritz.com

A significant portion of the landmark Gramm-Leach-Bliley Act enacted in 1999 ("Gramm-Leach") dealt with the privacy of consumer financial information in the hands of banks and other financial institutions. Federal bank regulators issued a joint rule on May 10, 2000, providing specific regulations to carry out the privacy provisions of Gramm-Leach.

The regulations basically require financial institutions to provide to their customers and, under certain circumstances, other consumers (those individuals who do not have a continuing relationship with the financial institution; for example, a person who uses an institution's ATM to access an account at another bank), certain notices outlining the privacy policies of the financial institution and the privacy rights of the consumer or customer. These notices include:

- an initial privacy notice
- an annual privacy notice
- an opt-out notice.

Disclosure of Privacy Policies Required

The initial notice is required to be provided to customers at the time the customer relationship is established, and to consumers if the financial institution intends to disclose non-public personal information about the consumer to a non-affiliated third party. Institutions must also provide to customers (but not consumers) an annual privacy notice. Each of the initial notice and the annual notice must accurately reflect the institution's privacy policies. Finally, institutions must provide to consumers and customers an opt-out notice that accurately explains the right of individuals to provide a direction to the institution that it not disclose non-public personal information about that individual to a non-affiliated third party.

Notices Must Be Clear and Conspicuous

The regulations require each of the initial notice, the annual notice and the opt-out notice to be "clear and conspicuous." To be clear and conspicuous, the notices must be reasonably understandable and "designed to call attention to" the nature and significance of the information in the notice. The regulations allow that the notices may be provided to customers and consumers electronically. However, the regulations stipulate that notices may be given electronically only if the individual to whom the notice is directed (a) obtains a financial product or service electronically and (b) agrees to receive the notice electronically.

Notices Must Be Easy to Find

If the notices are provided electronically, for example on a Web page, they must be designed in such a fashion as to use text or visual cues to encourage scrolling down the page, if necessary, to view the entire notice and to insure that other elements on the Web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice. In addition, either the notice must be placed on a screen that consumers access frequently, such as a page on which transactions are customarily conducted, or a link must be placed on such a screen which connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

The regulations require that all notices must be provided so that each consumer can reasonably be expected to actually receive it. In the electronic context, a reasonable expectation of actual notice is where the notice is posted on the Web site and the consumer is required to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service from the site. The regulations also note that it is an unreasonable expectation of actual notice to send a notice via electronic mail to a consumer who does not obtain a financial product or service electronically from the institution.

Regulations for Financial Institutions' Customers

For customers only, the regulations require that the initial notice and the annual notice must be delivered in such a manner that the customer can retain them, or obtain them later. This may be in writing or electronically. Electronic retention requires the notice to be available on a Web site (or a link to another Web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the Web site.

In connection with an opt-out notice, the consumer must be provided with a reasonable opportunity to direct the institution not to disclose non-public personal information about that consumer to a non-affiliated third party. In the electronic context, if a customer opens an on-line account and agrees to receive notices electronically, the regulations provide that a reasonable opportunity to opt out is afforded if the customer is allowed to opt out by any reasonable means within thirty days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

When Are the Regulations Effective?

The regulations became effective November 13, 2000, with compliance optional until July 1, 2001. Compliance with the regulations is mandatory from and after July 1, 2001.

Accordingly, institutions required to comply with the regulations should be in the process of preparing the forms of the initial privacy notice, the annual privacy notice and the opt-out notice; and, if that institution provides electronic banking services to its customers, it should be restructuring its Web site to comply with the regulations in the electronic context.

Christopher P. Daly is an associate in the Corporate and Banking Department at Farrell Fritz.

Handling Stock Options After Terminating Employees

By Andrew I. Cohen
acohen@farrellfritz.com

One of the legacies of the new economy is the adoption of stock option plans with employees at all levels of the company receiving options. While stock options have been a boon not only to employees previously denied meaningful incentive compensation but also to companies seeking to energize their workforce, the negative aspects of stock option compensation are increasingly obvious. Foremost among the negative effects of stock options is the enhanced risk of litigation by terminated employees.

While employees are often successful in exercising vested options upon termination, the number of claims for the value of unvested options have inevitably increased along with the growth in new economy layoffs. Several recent decisions highlight the uncertainty of the law in this area and the potential for terminated employees to immediately recover the value of unvested options, even if those unvested options might decline sharply in the future and be worthless.

In other cases, terminated employees have been able to point to a specific date at which a company's stock price was the highest and claim that, had they not been terminated, they would have exercised their options on that date. New economy companies are particularly exposed to liability resulting from claims for unvested stock options. In several notable decisions, courts have seemingly factored in the phenomenal growth of the companies being sued to justify awarding departing employees huge sums for their unvested options.

Companies can take several steps to minimize litigation and maximize the effectiveness of stock option plans:

- First, companies should have written stock option plans that employees must read and agree to. These plans, and the employee acknowledgment, should make clear that employment relationships are not modified by the stock option plan and employees are obligated to their original understanding with their employer, which in most cases is employment-at-will.

- Second, stock option plans and grants should be routinely examined and modified, as appropriate, to ensure that options are distributed to deserving employees.

- Third, departing employees should be offered appropriate severance packages taking into account the amount of potential damages that the departing employee could recover.

A general rule of thumb is that companies should give former employees approximately three-quarters of the value of options that might have vested during the year the employee was terminated. While the thought of offering terminated employees the value of options that might have vested during the year the employee was terminated or for later years might be unpalatable to many, the litigation savings, not to mention the public relations value, are substantial.

> ***...Courts have seemingly factored in the phenomenal growth of the companies being sued to justify awarding departing employees huge sums for their unvested options.***

Naturally, most litigation arises from companies with significant stock appreciation and/or potential for growth. However, companies with declining stock prices face similar issues. Employees feel doubly insulted when, upon receiving notification of termination, they are informed that they have only a specified time to exercise their valueless vested options (generally between 30-90 days) and that their unvested stock options will disappear altogether. Since amendments to stock option plans may require board of directors and shareholder approval, companies must pay severance through more traditional measures like cash payments or vacation credits.

In all circumstances, employers should be prepared to give terminated employees accurate information concerning their ability to exercise stock options. An employer who illustrates solid knowledge of the post-termination rights of employees, and who offers fair severance packages, is more likely to retain the loyalty and services of remaining employees.

Andrew I. Cohen is an associate in the Corporate Department at Farrell Fritz.

Workplace Privacy Programs

continued from page 1

companies to manage their liability and the safety and well-being of all employees?

Some of the topics that Wicks and Tomlinson covered were:

- How privacy issues in OSHA, Fourth Amendment searches and the New York Anti-Wiretapping Law affect workplace policies.

- Electronic monitoring of employees: how the pending Notice of Electronic Monitoring Act might function in the workplace.

- Security and privacy of company information on the Internet and Intranet.

- What is a reasonable personnel policy regarding applicant/employee background checks? A look at the issues, trends and laws, such as the Fair Credit Reporting Act, Driver's Privacy Protection Act, and Employee Polygraph Protection Act, that affect how human resource managers can investigate employees.

The "Long Arm" of the Law

continued from page 1

an Internet Web site to market and sell products or services.

Hsin Ten Enterprise USA, Inc. v. Clarke Enterprises, a recent trademark infringement action decided by Judge Shira A. Scheindlin of the United States District Court for the Southern District of New York, illustrates the real world impact of the issue. The case required Judge Scheindlin to consider whether the plaintiff, a New York manufacturer of an aerobic exercise machine, could properly maintain its New York lawsuit against one of the defendants, a Kansas company with no place of business anywhere other than Kansas. That defendant utilized an Internet Web site to market and sell exercise machines with a name similar to the one which the plaintiff used for its own product.

New York's "long-arm" statute permits a court to exercise personal jurisdiction over an out-of-state defendant where the defendant has transacted business in New York and the cause of action arises out of the transaction. Relying on this statute, Judge Scheindlin analyzed whether the Kansas defendant's Internet Web site activity provided a sufficient basis for exercising personal jurisdiction over it in the plaintiff's New York action. Judge Scheindlin concluded that it did. Personal jurisdiction over the Kansas defendant was appropriate, the Judge found, because its Web site enabled viewers in New York to purchase an exercise machine on line, download an order form, ask questions of an online representative, and even download an application to become an "independent affiliate" of the defendant for the purpose of selling its product, and because the defendant's sales of its product in New York were caused, at least in part, by its Web site activity. Calling the defendant's Web site activity "at the very least highly interactive," Judge Scheindlin found that it rose to the level of "transacting business" for purposes of New York's long-arm statute. And because the plaintiff's claim also rose out of that activity, the Judge concluded that personal jurisdiction over the Kansas defendant existed, therefore enabling the plaintiff to maintain its lawsuit against the defendant in New York.

But not all manner of Internet Web site activity can support a finding of personal jurisdiction over an out-of-state defendant. Whether it does depends on the nature and quality of the defendant's Internet Web site activity. The cases recognize three basic categories. And Judge Scheindlin summarized all three in *Hsin Ten*, reviewing when each could or could not provide a basis for conferring personal jurisdiction over an out-of-state defendant:

Passive Web sites: These primarily make information available to viewers but do not permit an exchange of information. These Web sites, which are analogized to advertisements, do not confer personal jurisdiction.

Active Web sites: These are Web sites where the defendant actively makes sales or enters into contracts over the Internet or transmits computer files to customers in other states. This type always suffices to confer jurisdiction over the out-of-state defendant.

Interactive Web sites: This type permits the exchange of information to the defendant and Web site viewers, and generally supports the finding of personal jurisdiction over the defendant.

The lessons of *Hsin Ten* and its kindred are straightforward. The Internet has created a new avenue for courts to examine in asserting personal jurisdiction over an out-of-state defendant. While the issue requires one to consider a particular state's long-arm statute, the outcome has real, practical consequences, in terms of decreased convenience and increased litigation costs, for the Web site-based business forced to defend a lawsuit out-of-state.

Michael J. Healy is Counsel in the Commercial Litigation Department, concentrating in Bankruptcy and Creditors' Rights.

Insurance Coverage

continued from page 1

endorsements expanding the scope of coverage to include some intangibles. For example, some policy endorsements define "property" to include "electronic data processing or electronically controlled equipment."

Equally important, a policy may exclude coverage for losses arising out of damage to computer systems or losses arising out of use of the Internet. Other provisions may exclude criminal acts from the scope of coverage. Only through careful analysis can it be determined whether coverage for computer-related losses is available under a traditional insurance policy.

Many insurance companies are now offering polices specifically designed to cover computer-related losses. For ultimate protection, such polices should be custom-tailored to the particular risks involved in the policyholder's business. The scope of coverage available varies with the type of policy purchased.

For example, a policy form being used by a consortium of insurance companies covers losses arising from damage to "Electronic Data," "Electronic Information Assets," "Electronic Computer Programs," and/or "Electronic Data Processing Media" resulting from a "Computer Virus," an "Attack," "Unauthorized Access" or "Unauthorized Use." These terms are defined in the policy.

Although there are several judicial decisions providing guidance as to the scope of coverage available under traditional policies, the new forms of insurance being offered to cover computer-related losses have not yet been subject to judicial scrutiny. This makes it all the more important that the coverage purchased be specifically tailored for the precise risks involved in a company's business. It is also important that the policy be analyzed by counsel to determine whether any "gaps" in coverage exist that might leave a company susceptible to potentially uninsured losses.

Eric W. Penzer is an associate in the Commercial Litigation Department.

Farrell Fritz Launches Second Generation Web Site

When we first put our "virtual office" -- www.farrellfritz.com -- on the Internet in 1998, our goal was to create a resource for clients and associates to learn not only about the firm but also about developments in the law and legal issues and trends. Since the time had come to update our site, we decided to give www.farrellfritz.com a design overhaul as well as add some functionality to the site. The Farrell Fritz Web site has hundreds of pages of articles, newsletters, press releases and other valuable information. How would clients and friends access this information in a quick and easy manner?

The answer: our very own search engine. It is located on every page of the Web site, in the "What's New" date box. Simply by typing in a combination of keywords, you will find any article, news story, press release, attorney profile, event or newsletter that has those keywords contained within the text.

Still can't find what you're looking for? Check the site map for an overall guide to the site. We have also added our new logo and artwork to create a site that is better organized, attractive and navigable.

The result? A more streamlined, useful and attractive site. If you have any comments, questions or suggestions, please let us know.

Among the new content features is our new Recruiting section, designed to help both job seekers and law school students find out more about Farrell Fritz. We encourage anyone to visit the section and learn more about what it is like to work for one of Long Island's finest employers.

And remember, if you want to receive techLAW via e-mail, visit www.farrellfritz.com and go to the In Print section, click Newsletters and click Subscribe to sign up for our e-mail list.

techLAW

techLAW is published quarterly by Farrell Fritz, P.C. Farrell Fritz, one of Long Island's largest law firms, serves large and small businesses, institutions, municipalities and individuals in corporate, banking, litigation, real estate, new media, land use, environmental, bankruptcy, tax, employment and trusts and estates matters. If you have any comments or suggestions, please contact our Editor, James M. Wicks.

EDITOR
James M. Wicks, Esq.
(516)227-0617
jwicks@farrellfritz.com

MANAGING EDITOR
Melissa Kane, Marketing Director
(516) 227-0623
mkane@farrellfritz.com

FARRELL FRITZ, PC
EAB Plaza
Uniondale, NY 11556
(516) 227-0700
www.farrellfritz.com