

**TENTH ANNUAL
NORTHEAST SURETY AND FIDELITY CLAIMS
CONFERENCE
OCTOBER 21 - 22, 1999**

**E-RISK PROTECTION POLICY
A NEW POLICY, NEW CLAIMS**

PRESENTED BY:

MEGAN M. MANOGUE
The Fidelity and Deposit
Company of Maryland

E-Risk Protection Policy A New Policy, New Claims

Activity on the Internet has grown rapidly over the last several years. Part of that activity includes e-commerce. As businesses and individuals transact more and more business online, banks and other financial service institutions are also participating in this rapidly developing sector of the economy. The activities engaged in by banks and other institutions online exposes them to new risks. In an effort to help protect them against that risk, insurers have developed and are continuing to develop new products to manage those risks. While this is an exciting development in the insurance industry, it also poses new challenges for claim handlers.

The Internet developed out of the efforts of researchers in the 1960s and early 1970s at the U.S. Defense Department's Advanced Research Projects Agency (ARPA) to try to link computers to each other. The researchers developed a system to allow computers to share data and exchange electronic mail. Eventually, students developed a way to use it to conduct online conferences. By the end of the 1970s, links developed between ARPANet and its counterpart in other countries.

Throughout the 1980s, this Internet expanded rapidly. Colleges, research companies and government agencies began to connect their computers to this worldwide Net. Eventually, some networks established to serve the academic community began offering services to nonacademic customers. Finally, in the early 1990s, a new way of organizing and interfacing information on the Internet - the World Wide Web - was created. The World Wide Web simplified navigating around the Internet so that all users could get around it.ⁱ

While the Internet expanded rapidly throughout the 1980s, its growth throughout the 1990s has been explosive. In January of 1990, there were an estimated 1 million Internet users.ⁱⁱ By 1995, there were an estimated 22 million users.ⁱⁱⁱ In early to mid 1999, the estimated number of Internet users stood at 130 million.^{iv} Even more amazing, the number of Internet users is expected to double next year.^v By 2005, the Internet is expected to support more than 500 million users worldwide.^{vi}

As the numbers of online users grows, so does the amount of business transacted online. As consumers become more and more comfortable navigating around the Internet, they are also more willing to conduct financial transactions over the Internet. Financial service institutions are joining the record numbers transacting business on the Internet. Many banks are now offering a number of services online, ranging from online banking, to brokerage activities to loan applications. In addition, the number of virtual or Internet banks continues to grow.

As financial service institutions expand the ways in which they engage in e-business and the professional services they offer over the Internet, they also expand the potential risks to which they are exposed. When financial institutions allow clients to access their

accounts online and to conduct other business over the Internet, they expose themselves to a variety of security risks. Hackers – individuals who attempt to hack in to a computer system – can cause a variety of problems. Typically, hackers are only interested in seeing if they can get into a system (with no intent of causing harm to the system). However, they can attempt to steal private customer information, intellectual property belonging to the financial service institution, and, by obtaining private customer information, they can eventually steal cash. Once a financial service institution allows customers to access account information over the Internet, the risk of someone else obtaining that information through the Internet exists.

Computer viruses pose another threat. Allowing employees to send and receive mail over the Internet also increases the possibility of employees receiving (and spreading throughout the company) viruses from the Internet. Some viruses, like the “Melissa” virus, can occupy so much of a computer network’s resources that they can effectively shut the network down. Other forms of malicious code can create havoc for computers. A Trojan horse consists of a program that appears to be useful and harmless but which has harmful side effects such as destroying data or breaking security on the system on which it is run. It is similar to a virus except that it does not copy itself as a virus does. A logic bomb, which can be downloaded along with a corrupted program, may destroy data, violate system security, or erase a computer’s hard disk.

Along with security issues, programming glitches can become a major problem when a financial service institution begins offering online services. Last April, some online banking customers who tried paying bills online received an error message that left them uncertain as to whether or not their transactions went through. The problem occurred because of a computer glitch involving CheckFree Holdings Corp., an online payment clearinghouse retained by many banks, and affected as many as 500,000 customers. Additionally, if a business is not adequately prepared for the volume of individuals accessing its site, it may become flooded and fail to provide access to all individuals trying to log on to it.

The Internet poses additional exposures for financial service institutions and other companies. While the Internet is a great source for information, it can also be a source for misinformation. Simply posting a website on the Internet exposes a company to certain risks. A hacker can attempt to access the website and alter the information presented on it. For a disgruntled employee, an unhappy customer, and a mischievous hacker, the Internet is an easy way to spread false and potentially damaging information about an institution. That kind of misinformation can damage a company’s reputation and its business. An employee, or even a programming error, can also unintentionally release information about the company or private information about customers over the Internet. The release of that kind of information can expose companies to lawsuits for liable, defamation, etc.

The Internet may also increase the risks to which financial service institutions are exposed by motivating them to expand the kinds of services they offer to their customers. For example, financial service institutions may offer services as Internet Service Providers to their customers. Or, they may offer hosting services. Hosting essentially involves leasing server space and web services to companies and individuals who wish to present a web or

e-commerce presence but do not wish to maintain their own servers. For an entity providing these services, an interruption of that service for any of the reasons previously mentioned may expose that entity to claims not only from the entity's customers, but also the *customers' customers*.

Another risk with these exposures is that the traditional insurance that many financial service institutions already have in place may not protect against all of the electronic risks created when doing business over the Internet. Traditional insurance deals with physical exposures, risks, and assets; it may not adequately protect against risks from electronic activity.

Because Directors and Officers Liability Insurance Policies do not usually provide coverage for the entity, they would not typically provide coverage for the exposures to the entity when it provides services over the Internet.

The Financial Institution Bond would not address many of the exposures arising through the Internet. The FIB does not typically address loss of intellectual property. It does not typically address the expense incurred in establishing the cause of loss (which would also assist an insured from preventing future losses). While the FIB may cover certain losses caused by employee dishonesty, it does not cover loss caused by employee error, such as a programming error.

Likewise, the Computer Crime Policy does not typically provide coverage for employee or programming errors. Even where it provides coverage for loss of electronic data or computer programs, that coverage is usually limited to the cost of duplicating such electronic data or computer programs. The Computer Crime Policy would not typically replace the asset value to the insured of that electronic data. It was not designed to address the new exposures resulting from conducting business over the Internet.

Because property and general liability insurance typically deal with physical damage or injury, they may not cover certain exposures related to electronic activity. For example, they may not provide coverage for loss caused by malicious code or programming errors. These kinds of exposures become much more significant when a portion of one's business is conducted over the Internet.

When Insurers began recognizing these new exposures which arise from doing business over the Internet, they began designing solutions to address these new exposures.

The Fidelity and Deposit Company was one of the first companies to come out with such a solution when it introduced its E-Risk Protection Program^{vii}. While a number of insurers now offer products that provide some form of protection for electronic activities, this paper will focus on E-Risk as one example of the kinds of solutions which insurers are providing.

Rather than simply offer an insurance product solution, the E-Risk program includes a risk assessment of an insured's electronic business exposures by trained professionals. These professionals will provide a thorough review of an insured's electronic business exposures. That includes a review of its electronic activities and security measures, and an examination of the causes of any previous security breaches. The review may result in

recommendations to bring an insured up to date in using the latest security measures in relation to its electronic business activities.

Using that assessment, F&D can also help insureds apply risk management tools to minimize and possibly eliminate risks exposed from the assessment program. That could include recommended training for employees or advice on how to institute security measures.

For any exposures remaining after the risk engineering described above, F&D will help insureds decide which risks to retain, avoid, finance or transfer. As part of the risk transfer mechanisms, the program offers insurance to uniquely cover the kinds of exposures created by the activities discussed earlier: activities (including e-mail) by employees on the Internet, customer access to account information and services over the Internet, private and public publishing on a Website, hosting clients' Websites, and selling products and services over the Internet.

The policy addresses certain covered causes of loss or "Loss Events" which include:

- unauthorized access to or taking of electronic data within covered electronic business systems.
- computer viruses and malicious code that damage data or covered systems.
- attacks to covered computer systems that take up so much of a shared resource that the insured loses access to its covered systems.
- the inability of an insured's covered electronic business system to provide proof of the origin and/or delivery of any message or data necessary to complete an electronic business transaction.
- for certain insuring agreements, unintentional programming and process errors made by authorized personnel resulting in claims by third parties.

The E-Risk policy contains a number of insuring agreements designed to protect against these risks including:

- *Loss of Business Income:* this coverage, for a covered cause of loss, replaces the insured's own business income and additional expense it may incur as a result of interruption of its business due to the failure of its covered electronic business systems resulting from a Loss Event. Part of the underwriting process includes determining a preset "Hourly Business Income" for each insured. The loss amount is then based on the time length of the business interruption and the predetermined "Hourly Business Income." Additionally, the policy covers the cost of investigating the reason for the loss of service. Determining the cause of the interruption of service can be critical to preventing further interruptions from occurring.

- Public Relations Expense:* this coverage is designed to help the insured rebuild its reputation from negative publicity resulting from the Loss Events noted above. The policy pays for the costs of retaining an approved public relations consultant to help the insured come up with a plan to minimize or prevent any damage to its reputation resulting from such negative publicity. The policy defines negative publicity as “information associated with or resulting from a **Loss Event** which is publicized through newspapers, radio, television or comparable print or broadcast media that has caused or is likely to cause a decline or deterioration in your professional reputation or which, in the opinion of a **Qualified Public Relations Consultant**, is likely to be so publicized to the detriment of your professional reputation.” This insuring agreement does not include any expenses other than those for the professional services of the qualified public relations consultant. This coverage recognizes the impact an interruption of service or other Internet exposure can have on a company’s reputation and is designed to minimize the impact of those kinds of problems to the company.
- Development or Replacement Coverage for Loss of Intellectual Property:* this coverage addresses the development costs an insured may incur from the loss of Intellectual Property due to a covered loss event. The policy includes in the definition of Intellectual Property, with respect to an insured’s covered electronic business systems, trademarks, copyrights, trade secrets, confidential business information, and software. This coverage includes replacement costs if software itself is lost or reimbursement of the unamortized cost of development if competitive advantage is lost through misappropriation.
- Interruption of Service Liability:* pays for certain claims made against the insured for e-business activity losses caused by or resulting from an interruption, delay, or suspension in the performance of an insured’s e-business activities due to the failure of its covered electronic business systems as the result of a covered loss event. If a third party cannot access an insured’s online services or perform financial transactions because the insured’s covered electronic business system shuts down, this insuring agreement may provide coverage for claims arising out of that service interruption. As more and more individuals and businesses rely on the Internet to conduct business and perform financial transactions, this coverage may become an important part of an insured’s risk management program. This insuring agreement is a claims made, duty to defend insuring agreement. Defense expenses are included within the limit of liability. For a bank allowing customers online access, acting as an internet service providing, or providing hosting services, this insuring agreement may provide coverage in the event the insured’s website shuts down and its customers file lawsuits alleging that they were harmed as a result of their inability to conduct financial transactions or conduct other transactions over the internet in a timely fashion.

- *Electronic Publishing Liability*: covers certain claims for libel, slander, product disparagement or trade libel resulting from Electronic Publishing. It includes coverage for certain claims for infringement of copyright, trademark and trade name in connection with an insured's Electronic Publishing activities. Like the interruption of service insuring agreement, it is a claims made, duty to defend coverage with defense costs included in the limit of liability.

The policy also includes a Difference in Conditions clause. This provision makes E-Risk the primary policy in relation to other policies which may provide coverage but were not specifically designed to address e-business exposures.

F&D developed the E-Risk Protection Program to address those risks and exposures created when a company enters the world of e-commerce and the Internet. Recognizing the varied exposures and the rapid rate at which technology continues to develop, F&D offers not simply an insurance solution but a risk management process. That process includes risk assessment, risk engineering, and risk transfer solutions. The E-Risk insurance product provides protection for a number of exposures that result from electronic activity.

As technology continues to make conducting business over the Internet easier, more individuals and companies will join those who have already participated in e-commerce. Providing solutions to financial service institutions and other customers for these kinds of exposures presents an exciting and new opportunity for insurers. It will also present new challenges for claims handlers as they become familiar with these kinds of policies and the claims that they cover. As technology develops newer, faster and more secure ways of conducting business over the Internet, the services provided over the Internet will likely increase. Additionally, the growing number of people using the Internet will also continue to demand that more services and products be available online. Unlike traditional insurance, products insuring electronic risks may undergo changes as the services that companies provide over the Internet increase and expand. Those of us handling the claims arising out of these kinds of insurance products will be challenged to keep up with these changing exposures.

ⁱ Worldwide Online Newsletter. Worldwide Online. 1 October 1999. Available: <http://www.wonline.com/newsletter/1999-01-1.html>

ⁱⁱ Quarterman, John S. *1997 Users and Hosts of the Internet and the Matrix*, Matrix Information and Directory Services. Available: <http://www.3mids.org/mn/701/pr790.html>

ⁱⁱⁱ Research Center Page. CommerceNet. 24 September 1999. Available: <http://www.commerce.net/research/stats/wwwpop.html#IPOP>

^{iv} Mellen, Sue. "Industry Experts, onlookers amazed by Internet Growth." Boston Business Journal, 11 June 1999, Vol. 19, Issue 18: 42.

^v Ibid.

^{vi} "Global Internet Usage to Grow, But Capacity Shortages Slow Development", Lightwave, May 1999, Volume 16, Issue 6.

^{vii} E-Risk is a trademark of The Fidelity and Deposit Company of Maryland. Statements made herein do not alter policy terms and conditions.