E-COMMERCE, E-PL & EMERGING RISKS
IN THE UNITED STATES:
NEW THREATS & NEW OPPORTUNITIES

by

Bernd G. Heinze
President, Beacon Management Group

Queens' College, Cambridge
6 September 2001

E-Commerce; E-PL & E-merging Risks in the United States: New Threats & New Opportunities[1]

By: Bernd G. Heinze, Esquire

President, Beacon Management Group[2]

We are privileged to have the opportunity to share with you some of the emerging risks and liabilities in the United States, which we believe will become more prevalent in the years to come. The advent and pervasiveness of e-commerce have expanded traditional exposures, and created new ones, which are now starting to find their way into the court system. We will examine some of the more important ones this morning, and provide a framework by which to evaluate and manage these new exposures.

Why focus on emerging American claims? Two reasons. First, sadly enough, one of the things we in America have perfected, is developing new ways to sue. The tip of a claims iceberg probably first surfaces in America – in California, Texas or Pennsylvania truth be told. Second, more and more American risk is being placed in the London

[1] The following paper was prepared as a general review of emerging claim and legal issues in the United Sates, and their potential effect on the insurance marketplace. The material is dated and any use of this document to assess liability must necessarily be supplemented with specific review of the particular facts and circumstances along with a review of any changes in the status of the law.

[2] Beacon Management Group is a trusted claims solutions provider, undertaking instructions in claim, litigation and audit management for domestic and international insurers, reinsurers, self-insured companies and investors conducting due diligence in mergers and acquisitions of other entrepreneurial ventures.

market. During the last two years, premium volume has increased substantially. Therefore, the opportunity exists to examine the forces behind the new exposures, and the opportunities to manage them appropriately.

Accurately predicting these new areas is not always easy. We can easily recall the time approximately two short years ago when the Market was quite concerned over a little problem called “Y2K.” And on New Year’s Eve we all watched the seconds tick down to midnight, wondering and waiting. Were our jobs still going to be there? Were our customers’ jobs still going to be there? If fire did break out from the hard drive disks being thrown into overload, would the sprinklers be able to extinguish them? How many elevators would become stuck in the high rises? Fortunately, other than mostly sue and labor issues, Y2k became less of an event exposure than had been feared.

Any predictions about future claims must begin with the current economy. Claims follow economic activity. The wave of environmental claims followed decades of heavy industry, albeit with some significant lag time for the manifestation and discovery of the pollution. Asbestos followed a boom in shipbuilding and construction of power plants. Mass tort claims like DPT/Benedictine, breast implants, formaldehyde insulation, tobacco and gun litigation, each followed periods of economic activity in the United States. Therefore, if any prediction can be accurately made, it is that the claims of tomorrow will follow the industries and economies of today.

The recent recessionary economic development in the United States has had a rippling effect on the marketplace. The dot com industries which drove the stock exchanges to record heights have now dwindled to such an extent that one wonders whether shareholder derivative actions against Directors and Officers can be far behind.

With this in mind, several areas emerge. We have identified some of the larger trends on matters we believe will occupy the diaries, bordereaux, and court dockets in the years to come. Namely, we shall concentrate this presentation upon:

- E-commerce
- Employment practice liabilities
- Directors and Officers claims
- Guns & Violence
- Health Care
- Construction defect and EIFS calims
- Asbestos & Environmental matters and
- The Restatement (Third) of Torts

The first burgeoning area is technology. Everyone is using computers. Business is being transacted at the speed of light. What some call the World Wide Web, is actually more analogous to the Wild, Wild West; a frontier so unstructured and without any barriers or enforcement mechanisms, that an untoward photograph, letter, remark or innuendo can be anonymously transmitted from the drafter to an incalculable number of people and websites.

What first started out as a way to access information on the world wide web, has turned in to a super-highway connecting millions of people and businesses portals. Starting with the mere ability to exchange e-mails and documents at the click of a mouse, long-distance telephone charges and mails can be avoided instant messaging techniques. Consumers can bid in auctions for items world-wide, share information in chat rooms, trade securities, and conduct business faster and more efficiently than ever before.

The movie 2001 wasn’t too far off when it predicted that computers would play a dominant role in our lives in the next millennium. Problems with computers have the potential to affect all aspects of our own economy, and those all around the world. The one thing that this tells us is that computer issues will continue to emerge as a major focus of insurance claims, simply because of the dominant place computers have in our society today.

The next area in which continuing growth and development has emerged is the field of employment practices liability. Sexual and racial harassment, wrongful termination, age discrimination and their related employment claims are on the rise, from the lurid disclosures involved in several infamous political scandals, sexual harassment in schools, and the newly introduced "failure to hire" claims. The inevitable pass-through to the insurance industry is just beginning.

Employee related claims are complicated and litigious and continue to surge impacting insurers and reinsurers alike. Not only have the number of employment-related lawsuits increased, but monetary award levels are also setting records. The Equal Employment Opportunity Commission reported more than 79,000 charges of wrongful employment practices filed with the agency in the year 2000. Public awareness of the laws has grown with the staggering damage awards granted to allegedly wronged employees. The current trend in suits can also be traced to the availability of meaningful remedies, and an increased access to jury trials in which the finders of fact and awarders of damage are more sympathetic.

Following the Private Securities Litigation Reform Act of 1995, the D&O insurance market continues to see increases in both claim frequency and severity. Average settlements in federal securities class actions have almost doubled since 1996 from US$6.93 million to US$13 million in 2000. Almost 50% of all D&O suits today are brought by shareholders alleging securities violations. Additionally, companies involved in a merger or acquisition are 50% more likely to encounter a securities claim. Many provisions of the PSLRA have increased litigation as the courts and counsel struggle with the interpretation the Act adding significantly to the defense fees in securities class actions. Additionally, in 2001, we can expect to see losses in D&O pick up from the failing technology and dot-com sectors.

Another are of emerging issues and opportunity are viewed in the municipalities and victims of crime filing suit against gun manufacturers and distributors. However, the issue remains alive as several appellate courts review the propriety of the failure to warn and other product liability issues.

Environmental enforcement actions and civil penalties imposed by the US Environmental Protection Agency have reached record-setting levels. Meanwhile, the law is moving in a direction not necessarily helpful to the insurance industry.

Medical malpractice and nursing home exposures have also begun a precipitous increase in presentation. With the recent passage of the national "patient's bill of rights," we expect the trend to continue. Claim severity in medical malpractice continues to increase due in large part to litigation trends and new liability theories. Additionally, nursing home losses have sky rocketed in recent years with the increase in patient rights law and public awareness.

These claims often allege neglect and abuse and seek punitive damages. The settlement and jury awards have been staggering and crippling to the nursing home industry as some insurance carriers have pulled out of some states.

The wave, or perhaps better phrased, "tsunami" of construction defect exposures are now emanating out of their birthplace in California to States like Nevada, Texas, Oklahoma, Florida, South Carolina and New Jersey.

Similarly, while property insurers have long dealt with issues of mold in homes and commercial buildings following significant water intrusion caused by severe storms and flooding, mold litigation has taken on a new twist and has become a new litigation field impacting homeowners, general liability, professional liability insurance, and other insurances available to contractors, landlords, school, municipalities and even architects and engineers.

These exposures assert a host of allegations including loss of use of the property, bodily injury to tenants and owners, mental anguish, illnesses and bad faith of the insurance carriers in failing to investigate the costs and make settlement necessary to make necessary repairs to the facilities. Mold can grow anywhere and easily on a wide variety of materials used in building homes, office buildings, and schools. We note that geographic areas susceptible to heavy rains and high humidity have also sustained concentrations of claim activity caused by mold.

We have also seen an increase in uninsured motorist insurance coverage exposures. Faced with two decisions from the Ohio Supreme Court which found (i.e., construed) coverage to exist in the underinsured and uninsured portions of private passenger auto policies, many auto insurance carriers in Ohio faced devastating losses and ceased writing commercial auto policies. Insurers are now faced with the potential of an explosion of uninsured/underinsured motorist claims. The situation has become so pervasive that the State Farm Insurance Company recently announced it was ceasing to underwrite business in New Jersey, in which it insured over 50% of the vehicles in the state. These two decisions greatly increase insurers and reinsurers financial exposures for auto claims.

Finally, the Restatement (Third) of Torts has recently been published. It has expanded the rights, remedies and responsibilities in product liability and design defect exposures. Risk utility analyses and definitions of “defect” or the “reasonable design alternative test” have been reconstrued, thus requiring a better risk analysis at the outset of a product being introduced into the stream of interstate commerce.

So, then, let us begin by breaking down the current industries and analyzing how they will provide exposures and opportunities for the insurance industry in the years to come.

The Impact of E-Commerce

At the turn of the 20th century, automobiles where still frightening animals, now they are named after them. Charles Lindbergh, a contemporary of the Wright brothers, was not yet flying. A short 27 years later, he flew across the Atlantic for some baguettes.

In the past 30 years, change has even been faster. The speed and efficiency of human enterprise have increased to the point we either no longer have time to do anything anymore, or we are "multi-tasking." We have gone from microwave cooking to processing information faster than we can handle it. Indeed the speed of technological change in the last 30 years has been unprecedented. The performance of microprocessing has doubled every 18-24 months since 1965. This phenomenon, known as Moore's Law, has brought CPU speeds in excess of a gigahertz (GHz = one billion clock cycles per second). Bill Gates postulated in his book *Business at the Speed of Thought* (1999), that the rate of technological change will continue at this pace and change the very nature of business. He was right.

So what does this mean for commerce, e-commerce and the business of insuring business? Nowhere has Moore's Law been more evident than in the area of e-commerce. While the World Wide Web did not even exist as a basis for interstate or global commerce a dozen years ago, there are now over 800 million websites. It is estimated that there will be over 7 billion by 2003. In 1998 U.S. businesses traded to the tune of about $50 billion by way of e-commerce. The U.S. Department of Commerce expects that number to surpass $3 trillion by 2003 and e-commerce is expected to reach some 6% of the Gross Domestic Product by 2005.

The advantages of e-commerce are obvious. Internet commerce allows a far broader reach and faster cycle than conventional sales markets. Access to electronic markets is simple, relatively inexpensive, and more efficient for the consumer. From the business end, this increased access leads to broader competition and an expansion of traditional markets for small businesses, as well as the elimination of cultural barriers and markets for large and small businesses, who can now add "globalization" to their business plans.

However, these new advantages also create new unknowns. These will lead to many novel issues that will have to be addressed by legislation, the courts, and even by business contracts addressing issues of jurisdictional interpretation and time of the essence provisions which are defined by the hour, rather than by a seasonal buying cycle.

These issues will in turn present risk. To assess and evaluate these risks we must dissect the nature of e-commerce, define the areas of uncertainty, and only then, will one be able to prudently evaluate the risk. Some of these issues include:

- Insufficient confidence in the privacy and security of electronic communications.

- Will the reach of the internet and its ability to advertise in one's own home, subject one to foreign jurisdiction

- Intellectual property claims from the form and content of a website.

- What coverage exists or should exist for these risks and how are the risks underwritten.

E-commerce commercial risks differ primarily in the area of anonymity. Neither the vendor nor the purchaser knows with certainty, with whom or what entity they are dealing. They don't see them, touch them and they therefore must rely more on faith. Unlike opening a physical outlet in a foreign country for example, the vendor may not study the customs and practices of the jurisdictions in which it sells through electronic commerce. That will increase its exposure.

Technical risks have also always been experienced. Machinery fails, delivery fails, the product fails. But now, we face hacking from within the e-business and outside the e-business; power outages causing loss of data; spamming and a host of other security issues. Like any factory, the impact of power outages can be mitigated with efficient backup of power. If the Internet becomes unavailable, the product may still be available, but the company simply cannot sell, and/or customers are unable to place orders necessary to keep their factories on schedule. Further, power outages increase the risk of security breaches. Merely keeping data up to date presents a risk with the speed of change. A factory or manufacturing plant can be hacked or entered only from the location in which it sits. An e-factory can be hacked from anywhere in the world. This distinction with traditional notions of limited risk and security is tremendous.

Security is therefore a far greater concern. Systems must be constantly updated and improved as hackers become more brazen and experienced. How secure is secure will depend upon the nature and importance of e-commerce to an assured's business plan. A revised basis of damage will also begin to appear, in terms of damage to profit, reputation, and customer base, in addition to the traditional business interruption damages.

Legal risks are profound as well. The uncertainties and the vagaries of the law and the Internet are profound. We will face major issues impacting jurisdictions and choice of law. Different countries, much less different states, will have different perspectives, interpretations, and regulations. Some issues will be determined in due course; others will remain under debate for years. Insurance underwriters and specialists will require a new brand of experienced specialists and intellectual capital to complement their e-commerce and e-risk products and exposures.

One of the most significant of the technology issues is whether the loss of electronic data constitutes property damage. We see the typical definition of property damage, here. In short, it constitutes: (a) physical injury to tangible property, including all resulting loss of use of that property, or (b) loss of use of tangible property that is not physically injured. But that being said, does electronic data constitute tangible property? Courts have disagreed.

- In *Seagate Technology v. St. Paul Insurance*, an assured manufactured allegedly defective disk drives which were incorporated into the claimant's computers, causing them to malfunction. The court held that the failure of the computers was not physical damage to tangible property, and thus, did not constitute "property damage" under the terms of the insurance policy.
- In *Retail Systems, Inc. v. CNA Insurance Companies*, a policyholder lost a computer tape that contained its client's data. The policyholder submitted the resulting claim to its insurance company which denied coverage on the grounds that the lost data was not property damage within the definition of the policy – physical damage to tangible property. The court ruled that because the data had been integrated into, and was located only on the lost tape, there was "tangible property damage" under the policy.

In addition to claims associated with software use, we can also expect many more claims against the growing number of businesses that engage in e-commerce. The overall e-commerce statistics are staggering. Within the next three years, consumer purchases on the Internet are expected to exceed $1.3 trillion, a figure which constitutes 9% of all U.S.

business trade and is more than the gross domestic product of Italy. In 1999 alone, there was a 100% increase in consumers who purchased products and services on-line. With respect to business to business commerce, over $50 billion in transactions occurred in 1998, and this figure went up to $138 billion in 1999. And with the number of web pages expected to exceed 7 billion by 2002, one can only guess what these financial numbers will look like a few years from now.

Of course, the use of e-commerce has raised new legal questions that have to be answered by legislators and by the courts. But it seems that electronic commerce has been advancing so rapidly that the laws simply cannot keep up with the technology. Just recently, the Congress took its first serious stab at regulating e-commerce in some time by passing the E-SIGN Act. This law ensures that an electronic signature on an on-line contract or other legal document will have the same legal enforceability as a handwritten signature on a piece of paper. But while this was a step in the right direction, there are clearly many more e-commerce questions that remain to be answered.

- How are local and national standards in laws enforced for Internet activity that is based on a URL address rather than a physical address?
- Do internet service providers have contingency plans for viruses like the "Lovebug" which interrupt service? For example, do service providers of online stock trading have a contingency plan to allow users to place trade orders in the event their website is unavailable? If not, who is liable for losses incurred by investors

who could not buy or sell a security because the website was down?

- Is an employer liable for an employee who uses the company computer for illicit activities or who uses the computer to sexually harass, or to racially discriminate?

Fundamentally, all of these are recognizable disputes and recognizable claims. However, the new electronic medium vastly increases insurers' exposure, and therefore raises the stakes.

Another area in which electronic technology may create a wave of new claims is that of privacy. In e-commerce, a tremendous amount of personal information is collected from consumers. Some websites post privacy disclosures. Whether they are accurate, whether they are followed, and what happens with the personal information collected is likely to give rise to invasion of privacy claims, some of which may be in class action form.

Electronic privacy is an issue as well in the workplace. For the most part, courts have upheld the rights of employers to monitor and read employees' e-mail. The financial services sector including the banking, securities, insurance, and real estate industries lead in electronic monitoring, followed by business and professional service providers (including lawyers) and wholesalers and retailers. This type of monitoring includes:

- storage and review of emails;

- recording and review of telephone conversations;
- storage and review of voicemail messages;
- storage and review of computer files;
- video recording of employee job performance;
- tracking telephone numbers called and time spent on calls;
- computer time and keystrokes entered; and
- video surveillance to counter theft, violence, or sabotage.

And finally, electronic technology may well have its greatest impact on insurers not as a result of any particular type of litigation, but rather by litigation, itself. The cost of litigation may increase dramatically as a result of electronic discovery. At this point, nearly every type of document is created electronically. There are, at present, approximately 81 million American Internet users and the projected number of e-mails to be sent in the year 2000 is 7 trillion. Only 30% of these electronic documents will ever be printed on paper. With the Federal Rules of Civil Procedure and the discovery rules of each state permitting the discovery of electronic documents, there seems to be little question that a majority of future litigation will contain electronic evidence. The problem with this, however, is that is poses a major financial burden for Underwriters and their assureds.

To begin with, the plaintiff's bar has undertaken aggressive efforts to gain access to the hardware and software of defendants. The American Trial Lawyers Association, for example, offers electronic discovery seminars. When ATLA members have left these meetings, they have gone on to make avid use of computer consultants in support of motions to permit onsite inspections of hardware and software. The effort required by Underwriters and their assureds to oppose these motions is remarkable. But it seems clear that burdensome and expensive electronic discovery is becoming a routine part of discovery in all types of litigation against defendants.

First, attorneys have come to realize that the delete function rarely makes a file unretrievable. In most instances, such action merely moves the file to another location. In addition, almost all companies have systems for downloading and storing network documents, drafts, and e-mails. Some companies even have systems for downloading and storing voicemail messages. It is clear that by the time a defendant turns over all of the requested e-mails, voicemails, and other types of data, the cost of discovery can be astronomical. In one case, for example, a federal district court ordered a defendant to produce 30 million pages of electronic data at their own expense, a figure that ran over $60,000.

While electronic discovery may not be an emerging claim, it is most certainly an emerging exposure. As has always been the case, Underwriters are often forced to settle meritless claims because the defense costs would be infinitely greater than simple payment of the claim. But in the years to come, the continuing use of electronic discovery may necessitate creation of new business modles and approaches to combat rising loss adjustment expenses, while keeping indemnity costs in check.

What is E-Commerce?

Stated simply, it is the process of doing business electronically. It entails some of the same components of traditional commerce and some that are not so traditional.

- It is a transaction, in which the parties intend that a binding agreement be formed through the use of electronic means, messages, responses and signatures.
- This is true, whether or not the parties contemplate the exchange of formal records to be reviewed and maintained by each.[3]
- This means access to retailers 24 hours per day, and 7 days per week; the theoretical ability to compare prices and product instantly, no matter in which what jurisdiction the respective consumer and vendor are in.
- Vendors advertise without regard to any geographical area and can distribute to any geographical area.

Thus, in traditional commerce we have storefronts, sales, written receipts, signatures, shipping, manufacturers, retailer, wholesalers, and people of whom the customer can enquire. In e-commerce, much of the same are evident, but we also see Internet backbones; ISP's; digital signatures; hardware and software makers; security vendors for the Internet infrastructure; commerce applications vendors; web-development software makers; search-engine software; on-line brokers; advertising networks; content aggregators; on-line travel agents; market makers; web retailers; subscription based sites; manufacturers selling online; entertainment and even professional services on line, all of which impact traditional notions of commerce and risk.

Identifying the E-Risks

The main areas in which e-commerce throws wrinkles into traditional commerce are:

- Writings – what happened to the Statute of Frauds? What constitutes traditional notions of “offer and acceptance” on-line?

- Proof – we all know how easily data can be altered. What is will happen to the best evidence rule?

- Jurisdiction – the Internet has no boundaries. If an employee of a manufacturer or service can accept terms and conditions of a sale anywhere in the world from his or her living room in New York State, while their laptop is connected via a high speed DSL modem line to the company’s mainframe in its home office in California, utilizing an Internet Service Provider located in Texas, can the employer then be sued anywhere in the world?

---

[3] Electronic commerce is contemplated in the Uniform Commercial Code, Article 2B Licenses

What Constitutes an Electronic Contract?

A full discussion of this issue is beyond the intent and scope of this presentation. However, we can touch upon them. Perhaps the greatest of all the differences between traditional and e-commerce, is in the area of written communications. While lawyers have often boasted a deal is not worth the paper it is written on, we now have to consider the value of the ether it is "written" on. These ether contracts can be formed by the exchange of e-mails, the completion of online forms supplied by the web host and significantly, by the simple act of downloading such things as online music, software or books when agreeing to stated conditions. Precisely when that contract is formed and what jurisdiction should interpret that contract is not as clear.

In traditional contract law, most states will find a contract complete when it is signed and dropped in a mailbox for return to the maker. It is not yet clear whether this timing is the same when dealing with the electronic contract, but if predictable, it will be.[4]

But now we have a new concern. Is it authentic? How much time is available to repudiate, if any? With the newly passed federal statute making digital/electronic signatures valid and enforceable, will the prospect exist for misappropriation of digital signatures being scanned and added to legal documents improperly? Under the rules of

[4] This assumes of course that the terms were not changed in any way by the party "accepting" the "offer."

evidence, documents must be authenticated before being considered in court. Under the existing Statute of Frauds, contracts dealing with land, those that can not be performed within one year, and contracts for the sale of goods with a value of greater than $500 must be in writing. How will e-commerce require the statute to be reformed?

Clickwrap Agreements are another way of creating a contract. These agreements are the list of terms and conditions to which we all click a button labeled “I Agree” without reading it. No signature is required, no negotiation is possible, no paper need be created. The fact that these are contracts of adhesion because one either buys pursuant to the stated terms or not, does not mean they are unenforceable. That factor will at best provide the buyer the opportunity to argue against enforceability. The courts will generally look to see if the weaker parties’ reasonable expectations were met and whether it is otherwise oppressive. Otherwise, these contracts are generally enforceable.

Jurisdiction

Generally, a business operating out of a physical location can only be sued in the jurisdiction in which it resides, does a significant business amount of business, or maintains sufficient “minimum contacts” with the jurisdiction. But when that brick and mortar business reaches deep into the ether by way of a web site, it increases the likelihood that additional jurisdictions will be appropriate for suit. Indeed, even the negotiation of a contract over the Internet makes it more difficult to determine which jurisdiction’s law will apply to resolve a potential dispute.

Traditional notions of contract law require that we look to the place of the last act necessary to make the contract and to then use its choice of law rule. That law in turn, more often than not, will require the judge to examine the state having the most significant interest in the contract. With the Internet, numerous different individuals in numerous different States and even Countries can simultaneously accept an offer. Thus, questions of international choice of law and even treaties with different countries can become involved in what was a simple question of jurisdiction.

Tort law is no simpler. Take the situation where a consumer, soon to be injured by the purchase of pharmaceutical drugs through an electronic supplier, (without a prescription no doubt), lives in California. The bad drug is located in New Jersey but the electronic supplier of the drug is located in Arkansas. The web transaction in the electronic sense probably went through servers in at least 15 other states. Alas, where does the injured party sue and which state's tort law applies? Again, we typically look to the jurisdiction with the most significant contacts or the jurisdiction with the most significant relationship to the dispute. Query therefore, can the pharmaceutical supplier and manufacturer be sued in every jurisdiction in which its product or good ends up?

Some general rules will help:

- How courts will treat jurisdictional issues will evolve and remain uncertain for some time to come.

- The more businesses use the Internet to reach into a given State to do business, the more likely the Court will find jurisdiction appropriate in that State.

- A web-site that is non-interactive; that is, one in which a consumer cannot place an order but is merely used to advertise, will not likely be enough to confer jurisdiction. Internet presence alone is not likely to be enough to confer jurisdiction. Simply gaining access to a business through a web site is not sufficient to result in jurisdiction. Actual business conducted through a web site may be sufficient.

- The more non-Internet contacts that exist within a particular jurisdiction, the more likely jurisdiction will be conferred. For example, toll free numbers, catalogues mailed to the State and advertising generally will increase the likelihood of jurisdiction.

At the end of the day, there is no simple answer to this question for the following two reasons. First, any determination of personal jurisdiction will be fact dependent. Second, the courts are not completely uniform on this issue. While some courts will exercise jurisdiction only where a website owner has directed significant attention and effort towards persons and businesses within their boundaries, other courts require far less action.

Despite some opposition, the courts tend to find no personal jurisdiction where a website owner has merely provided information upon request.[5] However, a minority line of cases holds that posting information on the Internet may, in and of itself, create jurisdiction in another state.

The pivotal enquiry is whether a web site owner, like the traditional business owner before him, has purposefully availed itself of the privilege of conducting activities in the forum state.[6] This determination is made by examining whether the relationship between the defendant, the cause of action, and the forum fall within the "minimum contacts" framework announced in *International Shoe, Co. v. Washington*, 326 U.S. 310 (1945), and its progeny.

Two traditional theories are used when evaluating a defendant's action for "purposeful availment" and/or "minimum contact": 1) Stream of Commerce Analysis; and 2) The Effects Doctrine. The leading court decision applying the stream of commerce theory held that "the placement of a product into the stream of commerce, *without more*, is not an act of the defendant purposely directed towards the forum state."[7] Thus, according to the Court, "[A] defendant's awareness that the stream of commerce may or will sweep the product into the forum state does not convert the mere act of placing the product into the stream into an act purposely directed toward the forum

---

[5] David P. Whittlesey, *Personal Jurisdiction and the Internet* (April 2000).
[6] *Hanson v. Denckla*, 357 U.S. 235, 253 (1958).
[7] *Asahi Metal Industry Co. v. Superior Court*, 480 U.S. 102 (1987) at 112, (*emphasis added*).

state."[8] In Internet jurisdiction cases, courts have frequently cited this "something more" requirement. As indicated earlier, this "something more" could include the simple posting of a toll free telephone number.

The leading Internet jurisdiction decision employing the Effects Doctrine, and one of the few federal appellate court cases concerning Internet jurisdiction, caused the Ninth Circuit to exercise jurisdiction over a non-resident defendant who registered the "Panivision" trademark as a domain name, and then attempted to sell the domain name to the trademark's owner.[9] According to the court, the defendant had "engaged in a scheme to register Panivision's trademarks as his domain names for the purpose of extorting money from Panivision. His conduct, *as he knew it likely would*, had the effect of injuring Panivision in California where [it] has its principal place of business."

Thus, under the Stream of Commerce Theory, jurisdiction may be exercised where the defendant has directed his website toward the forum by doing "something more" than merely placing the website on the Internet – *ie.*, something more than placing the website in the stream of commerce. And, under the Effects Doctrine, jurisdiction may be exercised where the defendant acted in a manner he knew would likely injure a party within the forum. Again however, no hard or fast rules exist. Both the jurisdiction and facts of the case can impact a determination of jurisdiction. Consequently, there are exceptions to the standards espoused above.

---

[8] *Id.*

[9] *Panivision International, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998)

For example, website owners should be aware of a minority of cases in which the court subjected a defendant to personal jurisdiction simply because the site advertised a toll free phone number, directed towards all states. Since the company consciously decided to transmit advertising information to all Internet users it knew that the information would be transmitted globally, and is thus hoisted by its own petard.

More reasonable courts have also adopted a sliding scale approach to determining jurisdiction. These courts look to the website to determine whether it is: 1) conducting business over the Internet; 2) whether it constitutes a passive web site, or 3) an interactive web site.

Passive websites, which merely post accessible information, generally do not provide grounds for exercising personal jurisdiction. An interactive site is best described as a site lying in the gray area between "doing business" and "passive websites". Examples may include sites that permit users to request franchise information, join a discount club, and purchase compact discs. These may be sufficiently short of doing business over the Internet to avoid personal jurisdiction around the world. That is, so long is the particular jurisdiction was not deliberately targeted without something more.

The issue of personal jurisdiction, while still in its infancy, will become more predictable as disputes are resolved pro-actively through contract terms and conditions at the inception of the the arrangement, as the courts establish common law rules, and as confusion surrounding the technology and medium continues to lessen.

E-Commerce Privacy and Security Issues

We began this paper by identifying privacy and security as “one” of the major issues impacting e-commerce. When someone walks into a store, looks at some goods, touches a lamp, or even makes a purchase, it is done anonymously. For the most part, even in those locations with high-tech video surveillance, there is no one following the consumer or visitor, taking notes on their shopping preferences or interests. Alas, the Internet has changed all that. As we browse on-line, our activities may be tracked in order to allow sellers to market their products more effectively. The on-line seller as such, must be concerned with and protect itself against claims of invasion of privacy.

Both consumer and seller should be interested in verifying activity on the Web. There are companies and organizations which specialize in reviewing and overseeing Web security policies on line. These entities provide differing verification procedures which provide consumers with the confidence that the site is what it purports to be; where the consumer can learn what information is being collected about them, and the assurance that personal information such as credit card numbers will be used for the purposes intended—a purchase.

Whether using these services will be a shield from liability for claims of violation of privacy or misuse of credit card information remains to be seen. Another open issue, is whether these entities might ultimately be liable to a consumer if a site breaches the security seals or certificates which are displayed. By analogy, we can look to an accounting malpractice claim by a party which relied upon an inaccurate audited financial statement to its detriment.

Other Legal Issues Arising Out of Use of the Internet.

The one certain risk in this rapidly changing world, is a business which fails to rise to the challenge of the Internet and its technology. The same holds true for the agent, broker, insurer and reinsurer of that business. The increased use of the Internet has and will continue to change the face of how Underwriters do business and importantly, the insurable risks of doing that business. Both state and federal legislation have been enacted to address various situations; intuitive solutions are available for others; while many other issues have been decided in what seems a counter-intuitive fashion.

Website Related Torts and Infringement

Web site torts (as distinguished from the contract issues briefly discussed above) generally fall into one of three categories: 1) advertising injury; 2) personal injury, and 3) bodily injury. The *Restatement of Torts (Third)*, tells us that advertising injury can take the form of trade libel, which occurs when a person publishes an untrue and disparaging statement of fact (as opposed to a simple opinion), which a reasonable man would foresee as adversely affecting a purchaser's conduct.

Personal injury on the Internet generally involves trespass or privacy invasion. Trespass occurs where one party "dispossesses" another of property. That "dispossession" includes destroying, barring access and intentionally interfering with property, and as such, trespass claims do lie for website disruption. Invasion of privacy can take four general forms:

- Intruding upon a person's solitude in a manner that a reasonable person would find offensive.
- Appropriating the name and likeness of another for economic benefit.
- Creating "unreasonable publicity" about another person's private life.
- Publicly casting another in a false or misleading light.

The most common types of specific actions are:

Defamation, Libel, Slander and Disparagement - Though closely aligned, each are nonetheless different.

- "Defamation" describes false communications to third parties that damage a person's reputation.
- "Slander" is defamation by spoken word, while "libel" is defamation by written word.

- "Disparagement" is the false and malicious representation of another's interest in property.
- "Trade libel" and "product disparagement" is directed towards a business' goods or character, as opposed to the reputation of a person. Mere general statements of comparison, declaring the defendant's goods are the best on the market and are superior to the plaintiff's (i.e., "puffing"), are privileged as long as they contain no specific assertions of unfavorable facts reflecting upon the other product.

Violation of Privacy or a Persons Right of Privacy - There are four types of conduct that infringe upon a person's right of privacy: 1) intrusion upon a person's seclusion or solitude, or into their private affairs; 2) public disclosure of embarrassing private facts about the person; 3) publicity that places the person at false light in the public eye; and 4) appropriation of a person's name or likeness for the wrongdoer's advantage.

Unfair Competition - Unfair competition, based primarily on the common law, is generally concerned with protecting company names and symbols from competitors who might copy them in order to steal business. The classic case of unfair competition involves the "passing off" or "palming off" of one's goods, services or ideas as those of another.

Infringement of Copyright - The *Federal Copyright Act, 17 U.S.C.A. §101 et seq.*, provides federal copyright protection for "original works of authorship fixed in any tangible medium of expression." The Copyright Act preempts all legal or equitable rights created under state statutes and common law equivalence. A work is protected under the act from the moment it is fixed in tangible form. Infringement of a copyright is the violation of any of the exclusive rights of the copyright owner, including the rights of reproduction, adaptation, distribution, performance or display. An example of a copyright slogan or title would be "Just For The Taste Of It" and "Big Mac".

Online music access from websites offering music sharing software has recently been challenged by the record industry in the now well known *Napster* litigation. The lower court in Napster found an internet music provider could not defeat a copyright infringement action by the music industry by classifying itself as merely a "passive conduit." The appellate court affirmed the ruling and has substantially eliminated future sharing of music and copyrights free of charge.

Patent Infringement - Patents are protected under the Federal Patent Act (35 U.S.C. §101 et seq.). Federal courts have exclusive jurisdiction over patent infringement cases. In order to obtain a patent, an applicant must show utility, novelty, and non-obviousness. Under 35 U.S.C. §271, a patent can be infringed either literally, under the Doctrine of Equivalence, or by the inducement of another to infringe a patent.

Literal infringement occurs where the wrongdoer's property is a clear imitation of the patented property in both form and function. Infringement occurs under the Doctrine of Equivalence when a product performs substantially the same function or work, in substantially the same way, to obtain substantially the same result as the property protected by the patent. Inducement to infringe a patent arises when one causes, urges, encourages, or aids another to infringe a patent.

Trade Secrets - A trade secret is information that is not known to others and that gives its owner a commercial advantage in the industry over competitors. A trade secret may consist of any formula, pattern, device, or compilation of information, which is used in one's business, and affords an opportunity to obtain an advantage over competitors, who do not know or use it.

Trade Dress - Trade dress broadly refers to the overall image of a product. It is the visual image by which a product or service is presented to the consuming public. It is more than the appearance or color, but rather is both the total image and overall appearance and the manner in which goods or services are presented to prospective purchasers to indicate source. Trade dress protection is of a descriptive image or appearance occurs when the descriptive mark takes on a secondary meaning to establish a customers association with a source.

The *Lanham & Federal Trademark Act*, 15 U.S.C. §1051 et seq., establishes a cause of action for unregistered trade dress infringement and seeks to protect the public from confusingly similar marks or product appearances. A claimant must prove: 1) that the two competing products are similar enough to create a likelihood of confusion among the consuming public; 2) that the appropriate features of the allegedly copied product are nonfunctional; and 3) that the trade dress is either inherently distinctive or has acquired a secondary meeting. Some experts in the field predict that trade dress will take on new life and significance in the rapidly developing area of Internet law.

Trademark Infringement and Dilution - A trademark is any word, name, symbol, or other device used to identify or distinguish goods from those manufacturers, sold by others, to indicate the source of the goods. § 43(a) the Lanham Act, Federal Trademark Act, provides for a federal system of registration of trademarks. Federal registration provides constructive notice of the individual's claim of trademark rights and is evidence of the validity of a mark. Common law trademarks are still recognized in the United States, notwithstanding the Federal Trademark Act.

Tortious Use of Links, Frames, and Metatags

While we may believe any person or organization would love to have a free method of advertising its wares by way of a link from another site, that is not always the case. As such, both website owners and operators should be mindful of potential liability arising from linking activity. One can be liable for: 1) providing an unauthorized link to another website; and 2) inserting another company's tradename or mark in a metatag.

There are two types of hypertext links ("links"). Hypertext Reference (HREF) links are pieces of text, differentiated by color or formatting, that lead users to a completely new URL address. "Image" (IMG) links, on the other hand, permit users to view content from another website while remaining at the very same URL address.

Because HREF links increase the number of "hits" for a linked-to site, they are generally considered advantageous. Thus, the prevalent view as suggested above, is that website owners implicitly consent to HREF links to their sites. But at best, this "implied license" provides only a defense against claims arising from a website's unauthorized HREF links. Thus, for example, if a pet shop's website provides a link to a dog groomer's website (as a customer service), such action is likely protected. However, if a website expressly prohibits unauthorized linking, the implied license may be lost. In either event, the implied license might not extend to competitors.

While HREF links are generally considered a "safe bet", not so for IMG links. Consider, for example, *Playboy Enterprises Inc. v. Universal Tele-A-Talk*, 1998 U.S. Dist. LEXIS 17282 (E.D.Pa. 1998). The *Tele-A-Talk* website repeatedly used the Playboy name and "bunny" trademark, and provided an unauthorized IMG link to the official Playboy site. The court's finding for plaintiff comports with the general rule that the use of another's tradename, mark, or logo as a link icon can result in trademark infringement.

In addition to infringement, "dilution" of a trademark is an important issue. "Dilution" is the just that, the dilution of a famous mark's capacity to distinguish its owner's goods. Unauthorized linking can form the basis for dilution of one's mark by "associating", one site with another, thereby potentially tarnishing the image of the linked-to site. Secondly, a so called "deep link" (a link to a page beyond the homepage) may distort the overall feel of the linked-to site and thus form the basis of a "dilution" claim.

Use of Frames

As with IMG links, the unauthorized use of "frame" links can also lead to trademark liability. Frame links are often utilized by metasites, which provide collections of links. The "frames" allow viewers to divide the metasite into multiple, scrollable windows that operate independently of one another – much like picture-in-picture television. Thus, users view another site's content without leaving the metasite itself.

Metatags - Search engines rank a website according to the frequency at which key words appear within its metatags, text, URL, and domain name. A metatag's content is ordinarily unseen by the user. Most companies include only their own trademarks and other appropriate descriptive words in their website metatags, but some use the trademarks of competitors in order to attract potential customers.

Generally speaking, the unauthorized use of a tradename within a metatag is actionable for direct and contributory trademark infringement; trademark dilution; tortious interference with contract, and unfair competition.

This is not to say that another's tradename or mark may never be included in a metatag without authorization, just that great care should be taken. For example, an automotive trade magazine may include the trademark "Volvo" if the site is providing a review of the automobile. This exists as an exception first because the publication is not attempting to divert business from the trademark owner and second, persons running a search engine enquiry for "Volvo" are not necessarily looking for automobile dealers.

The Effect on the Insurance Product and Industry

Clearly, traditional insurance products cover some of the risk, such as CGL, E & O, and fidelity bonds. But there is so much more. And how will traditional reinsurance covers respond? Like any form of commerce, e-commerce presents commercial, technical and legal risk. Those risks, while somewhat the same, will in different packages.

<u>Underwriting the E-Commerce Risk</u>

The insurance underwriter must be aware that as in most commerce, there will be traditional risks including commercial risks, technical risks and legal risks. As explored above however, the underwriter has much more to consider. On the commercial side, an underwriter should be well informed of the commercial risk management of an insured. Is the insured a merchant? Is that merchant constantly failing to fulfill orders? Are employees happy? What type of product is being sold?

With regard to technical issues, the underwriter must determine and be familiar with who the parties are to the transaction. If the security or any other issue is outsourced, the 3rd party must be investigated and analyzed for competence. What protection is there for virus infection? How often is it updated? How frequently does hacking occur in that industry and in that business specifically? What type of information is stored? Is it the type of information that is likely to be hacked such as credit card numbers or bank account information? What type of monitoring is performed by the business and how often? Is the industry one that is likely to be hacked for commercial gain or one that is hacked merely for gamesmanship? How visible is the risk? Is it Microsoft or XYZ, Inc?

In this entire exercise it is important to the focus of insurance must shift from the protection of physical property and personal injury to a world of intangible property in many ways. The world still manufactures products, but we now also manufacture, sell, distill, store, impart and share information, and lots of it. It is an economy based on information and knowledge and the speed by which that knowledge can be exchanged and marketed. It is incumbent upon the insurance industry not to keep pace with this change, but to be ahead of the trends and to offer security in creative, non-traditional fashions.

Specifically, the industry must now more than ever before concern itself and focus on non-physical losses, losses which cannot be seen or touched. Advertising, intellectual property claims and losses of data base information are just a few areas. While many standard insurance products will address some of this risk, the underwriter must re-evaluate – in due diligence fashion - the exposure presented by that risk and in turn, its pricing.

The traditional insurance forms were drafted decades ago, before the Internet phenomenon. Traditionally, insurance products have reacted in large degree to past or previous events. The opportunity is to now reverse that trend and address changing business and market conditions, and afford creative niche or manuscript covers.

For instance, all-risk forms were developed in the early 1960's to encompass other physical risks, not just the traditional physical named perils of fire, wind, and hurricane. Events and even the business cycle today, change not every decade, not every year or even every month. Significant events impacting the insurance product happen daily and faster. The more an assured company interacts with third parties, the more likely it will be liable for some alleged wrongful act to occur. It may be an innocent exchange of goods or services for monetary consideration, but may be viewed quite differently by an aggressive plaintiff attorney. It only stands to reason that if a company can simultaneously sell to buyers throughout the world, somebody will become disenchanted with something, sooner than usual. That risk is not the same as that faced by the brick and mortar business. A small example: a contract is negotiated with a vendor. Before the contract is even signed, that vendor has been acquired by another company with different controls and protocols in place. Drafters of insurance products must constantly address and keep up with that rate of change.

Similarly that company's advertising risk is greater; the risk to computer crime is obviously greater; the exposure to economic loss is logarithmically increased; and business interruption losses can multiply exponentially to those we have traditionally seen. Thus, while some of the risks will be of the same nature they will not be the same level of risk. Just as the law has not always caught up to the realities and vagaries of e-commerce, neither has insurance coverage.

<u>What are the Insurance Needs of Internet or E-Commerce</u>

There is potential coverage under comprehensive general liability policies ("CGL") for many Internet and web site related torts. Some insurers have also recognized the need to provide new coverages addressing the new forms of technology. Both new and traditional coverage will ultimately need to be carefully examined in the areas of First Party Property, Commercial General Liability, Directors and Officers Liability, Errors and Omissions, Employment Practices, and Surety and Fidelity covers.

Regardless of how fireproof a firewall may be or how secure a lock may appear, there will be losses and a risk of damage to property, no matter how unforeseeable it presently may appear. This fortuitous direct physical loss of property is why there is property coverage. The law is still evolving on the issue of whether "software", access to the Internet, or other forms of programs or magnetic data qualify as covered property.

In the context of traditional business direct physical loss meant one thing. Traditional business derived income from the quality of its machinery, equipment, buildings and goods. It is this business concept that existed when the current policies were written and the exposures considered. E-businesses however, maintain assets in the form of software programs, magnetic data, networks and Internet access. Their most important asset is not the machinery and equipment. Instead it is information stored magnetically and the company's ability to access the Internet. This represents its main source of income. It will likely be this distinguishing factor that will drive the ultimate interpretation of what qualifies as covered property, and which events constitute covered risks of loss.

While Underwriters will almost certainly argue that the rearrangement of electrons (which is what happens when software is damaged) cannot possibly qualify as covered property contemplated years ago, current trends would suggest that with the passage of just a short amount of time, electronic media in almost any form, will be considered covered property unless it is very specifically excluded.

In this respect, Underwriters may wish to consider augmenting Electronic Data Processing Coverage beyond the current forms to address some these issues. In this way, the opportunity to calculate risk as well as underwrite and derive premium from the assumption of an intended risk will be afforded. Further, a more comprehensive evaluation can then be made as to the proper premium to be charged, the amount of retention underwriters wish to subscribe on the slip or retain net of reinsurance, and how best to structure the outwardly ceded allocation spread of the risk.

Advertising injury related torts are currently the largest category of technology torts and carry the potential to trigger advertising injury liability coverage under Section B of the standard (CGL) policy, which provides coverage for that which the insured becomes legally obligated to pay "as damages" because of personal and advertising injury" caused by an "offense" arising out of the assured's business. The definition of advertising injury includes many of the content related claims which could be asserted as a result of on-line activity, including libel, product disparagement, violation of privacy rights, , "use of another's advertising idea", trade dress, and copyright infringement. One traditional advertising injury theory is that misappropriation of an advertising idea is the wrongful taking of the manner by another advertises its goods or services. That theory applies equally well to the Internet as to conventional advertising mediums.

One commentator has suggested the "advertising injury" provisions of traditional policies do not apply well to defamation, copyright, trademark infringement or invasion of privacy claims, because the provisions require liability to arise from and be caused by an "advertising activity".[10] This thesis holds that much of what is on a website is not advertising activity, rather it may just constitute a "virtual store". He also notes that the Insurance Services Office ("ISO") has further restricted provisions by requiring alleged offenses to occur within the advertisement itself. Thus, while some parts of the site may result in a claimed advertising injury and coverage, much of the site may not be considered part of an advertisement.

Regardless of the position taken, it is clear the Internet and software technology will lead to new questions and opportunities concerning "advertising injury" coverage.

New technology from Epidemic Marketing, an e-mail marketer in Denver, Colorado presents a unique prospect for Underwriters. Epidemic sells software capable of embedding graphic advertisement links in e-mail messages. Over 8 billion e-mail messages are transmitted daily. E-mail also has the potential to generate numerous tort actions, especially defamation and invasion of privacy claims. If e-mail advertisements receive coverage under "advertisement injury" provisions, Underwriters may face a tremendous potential risk dwarfing the exposure presented by nursing homes and asbestos.

Directors and Officers liability insurance should not be ignored in the context of e-commerce. As we have referenced, the risks and exposures presented by e-business are unknown. It can only follow therefore, that D & O exposure is equally uncertain.

[10] Adam H. Fleischer, Advertising in Cyberspace, The Changing Face of Injury (May 2000) p. 55.

Similarly, Fidelity Surety and Crime insurance is a must. Moreover, the thefts under these policies will or may involve theft not of money or goods, but the use of fiber optics and other tools of e-commerce to gain monetary advantage. In such a situation, we must ponder whether there is a loss to the insured company that can be measured.

Whether there will be coverage for a particular e-commerce tort will of course depend upon the courts' interpretation of these new technologies, the language of the policies and the specific facts and circumstances. However, while there will be speculation as to coverage, there is little doubt there will be related litigation at least until there is a body of law to guide insurers and insureds in evaluating claims.

In the interim, we have seen the value of Underwriters and claim professionals utilizing the services of a single claims solutions provider. The benefit arises in the pre-binding stage, as Underwriters consider the nature, type and extent of cover to which subscription will be made, and through the strategic alliance, can be better prepared on the appropriate terms, conditions, exclusions and other endorsements to be offered in the insuring agreements based upon virtual daily changes in the regulatory environment and common law in the various 50-states.

Similarly, claim professionals have traditionally spent time and dollars with law firms and qualified attorneys to supervise the "process" of portfolios of business in the US. The opportunity now exists to utilize the alliance between the claim professional and the claims solutions provider to advise and assist the claims department on the management of claims to the best financial and total loss cost outcome, with compensation tied directly to the results achieved.

The New Regulatory Environment

Closely associated with the dramatic changes in e-commerce are a number of privacy-related claims involving matters like e-mail monitoring and invasion of privacy. But privacy may become an even bigger issue in light of the newly enacted Gramm-Leach Bliley Act. This financial services legislation breaks down the traditional barriers between commercial banking, investment banking, and insurance sales and underwriting.

An Introduction to the Privacy Requirements and Notice Provisions of the Gramm-Leach Bliley Act

The following materials are intended to serve as a guide to insurance professionals in responding to the privacy requirements of the Gramm-Leach-Bliley Act and its implementing regulations. These include an annotated model privacy notice and copies of a broad range of background documents. There are, of course, no substitutes for legal counsel, particularly for companies with complex organizational structures or information-sharing arrangements. In addition, since each state has separate compliance standards on implementation of the Act, the specific regulations of each state in which the agency or insurance company has offices, in which its producers transact business, and in which the policyholders are located, will all need to be examined in order to ensure proper compliance.

<u>The Gramm-Leach-Bliley Act</u>

The Gramm-Leach-Bliley Act became law on November 12, 1999. The Act, which was years in the making, started life as a series of bills to reduce the barriers between the banking and securities businesses, and then the banking and insurance businesses. However, increased consumer concerns about privacy made it impossible to enact any financial services reform legislation in 1999 that did not increase consumer privacy protection. The resulting Act includes broad requirements intended to safeguard nonpublic personal information. The Act's privacy requirements are not limited to the banking, securities and insurance businesses but, instead, apply to almost every business engaging in financial activities. The Act refers to these businesses as "financial institutions," but the term includes many smaller businesses that are far from the usual concept of an "institution."

The Act assigns responsibility for implementation and enforcement of the privacy provisions to a number of regulators, with the Securities and Exchange Commission responsible for brokers, dealers, investment companies, and registered investment advisers. Investment advisers that are not registered with the SEC, however, are subject instead to the Federal Trade Commission's rules under the Act. All of the responsible regulators (except for some state insurance departments) now have adopted regulations to carry out the purposes of the Act. All of the federal regulations went into effect November 13, 2000, but compliance is not mandatory until July 1, 2001. The SEC regulation is called Regulation S-P; the FTC did not give its regulation a special name.

The essential outlines of the regulations are mandated by the Act, which already contains specific requirements for the protection of consumer privacy. Under the Act, financial institutions may not disclose to a nonaffiliated third party any nonpublic personal information, unless the financial institution has provided to the consumer a notice of the institution's privacy policy and the consumer has not directed that information not be disclosed. The regulators, acting in accordance with the Act, have consulted and coordinated with each other in proposing rules implementing the Act's privacy provisions, and each regulator's proposal takes a similar but not identical approach.

Scope of the Regulations

The Act's privacy provisions apply to virtually every business engaged in financial activities that collects nonpublic personal information about individuals who obtain financial and insurance products, or other services primarily for personal, family, or household purposes. Information about companies, or about individuals who obtain financial and insurance products or other services primarily for business, commercial or agricultural purposes, is not protected. Regulation S-P applies to the financial institutions for which the SEC has enforcement responsibility under the Act, namely, brokers, dealers, investment companies, and other investment advisers that are registered with the SEC. The FTC's privacy regulation covers those financial institutions that are not otherwise assigned a regulator, and this includes U.S. broker-dealers and investment advisers that are registered only at the state level or that are altogether exempt from registration.

To the extent that financial institutions and/or insurance entities provide insurance products that are not securities, they are subject to regulation by state insurance authorities rather than the SEC. Variable insurance products, however, are both insurance products and securities, and therefore, subject to both Regulation S-P and state insurance regulations, as are insurance company separate accounts that are "investment companies" under the Investment Company Act of 1940.

Copies of the materials noted below follow:

- A Model Privacy Notice with Annotations
- A Model Short From Privacy Notice with Annotations
- A Summary of Provisions of the Financial Services Modernization/Gramm Leach Bliley Act A Summary of the Congressional Conference Summary Report for Title III – Insurance, of the Act
- A copy of Title III – Insurance, of the Act
- A Summary of the Congressional Conference Summary Report for Title V - Privacy, of the Act

If insurance products are sold, the insurer and/or issuing company will also be subject to state insurance regulations. The National Association of Insurance Commissioners has promulgated a model state regulation. Most states have now adopted a regulation based on the NAIC model.

The state of Texas has also specifically addressed the Act's applicability to managing general agents. Texas Insurance Code Article 21.07-3 is ruled to be preempted by Section 104(d)(2) of the Gramm-Leach-Bliley Act to the extent that the Insurance Code does not contemplate that a depository institution, financial holding company, financial subsidiary or operating subsidiary of a depository institution may be licensed as a managing general agent in Texas. As a result of this preemption, any of these entities may obtain a managing general agent's license by complying with the statutory requirements outlined below.

> The provisions of Texas Insurance Code Article 21.07-3 Section 4(a) requiring each applicant for a managing general agent's license to be a resident of Texas is preempted as applicable to a depository institution, financial holding company, financial subsidiary or operating subsidiary of a depository institution. The preemption results from Section 104(e)(3) of the Gramm-Leach-Bliley Act, which provides that no state law may effectively prevent a depository institution or affiliate from engaging in insurance activities authorized by the Act. As a result of this preemption, a depository institution, financial holding company, financial subsidiary, or operating subsidiary of a depository institution may obtain a managing general agent's license in accordance with these guidelines without regard to the Texas residency requirement in Article 21.07-3 of the Texas Insurance Code.

The provisions of Texas Insurance Code Article 21.07-3 Section 5(h) prohibiting a bank, bank holding company, or a subsidiary of either entity from owning a managing general agency is preempted by Section 104(e) of the Gramm-Leach-Bliley Act. This ownership prohibition is preempted because it discriminates against a depository institution by adversely impacting the depository institution when compared to other persons providing the same products and services that are not depository institutions.

As a result of this preemption, a depository institution, financial subsidiary, or operating subsidiary of a depository institution that is properly licensed in Texas as a managing general agency may own a licensed managing general agency. The agency or carrier owned in whole or in part by such entity must be licensed according to the requirements set out in the Texas Insurance Code, except that the residency requirement in Article 21.07-3 is preempted with respect to the depository institution, financial subsidiary, or operating subsidiary that is a shareholder, member, or partner of the agency or carrier.

NCOIL has also weighed in to establish its own Model Regulation. One way that the NCOIL Model differs from the NAIC Regulation is that it provides for basic protections for health information, while the NAIC Regulation addresses medical privacy in greater detail. The NCOIL Model requires an "opt in" provision for the sharing of health information solely for the marketing of services or goods for personal, family or household purposes.

The NCOIL Privacy Task Force decided to wait for the release of the final Health and Human Services (HHS) "Standards for Privacy of Individually Identifiable Health

Information” before establishing a position on medical privacy. The recently released federal standards implement the privacy requirements outlined under the Administration Simplification subtitle of the Health Insurance Portability and Accountability Act (HIPAA). NCOIL is currently reviewing the standards. The NCOIL Health Insurance and Workers’ Compensation Insurance Committees, in conjunction with the Privacy Task Force, are charged with establishing a position on medical privacy for 2001. In addition, the National Conference of Insurance Legislators has adopted a Financial Insurance Privacy Protection Model Act for those states that will need implementing state legislation. Many other states have adopted their insurance laws or regulations at this writing, and follow the NAIC or NCOIL model.

<u>Who Must Receive Privacy Notices</u>

A central distinction in the regulations is the difference between a “consumer” and a “customer.” The significance of the distinction is that a financial institution must give a “consumer” who is not a customer the required notices only if the institution intends to disclose nonpublic personal information about the consumer to a nonaffiliated third party (other than for certain legally allowed purposes). By contrast, a financial institution must give all “customers,” at the time of establishing a customer relationship, a notice of the institution’s privacy policy. All customers are consumers, but not vice versa.

Under the regulations, a *consumer* is an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes. An individual who provides nonpublic personal information when seeking to obtain insurance, financial, brokerage or advisory services is a consumer, even if no insured, brokerage or advisory relationship is established. The reasoning is that a “financial product or service” includes the evaluation of information an individual provides to the financial institution in order to obtain some other financial product or service. On the other hand, an individual who provides his or her name, address, and areas of insurance interest in requesting information or a brochure is not a consumer.

A *customer* is a consumer who has a customer relationship with the institution, that is, a continuing relationship between a consumer and an institution under which it provides one or more financial or insurance products or services to the consumer that are to be used primarily for personal, family, or household purposes. In general, a customer relationship is established in situations when a consumer typically would receive some measure of continued service following, or in connection with, a transaction.

<u>Nonpublic Personal Information</u>

A central definition of both the Act and its implementing regulations is "nonpublic personal information," which is the private information protected by the Act. The Act defines nonpublic personal information to mean personally identifiable financial information provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution, but not including publicly available information.

Personally identifiable financial information, under the regulations, means any information:

(i) a consumer provides to a financial institution to obtain a financial or insurance product or service;
(ii) about a consumer resulting from any transaction involving a financial or insurance product or service between a financial institution and a consumer; or
(iii) a financial institution otherwise obtains about a consumer in connection with providing a financial or insurance product or service to that consumer.

In essence, the rule treats any information as "financial" information if a financial institution obtains it in order to provide a financial product or service, even if the information is not "financial" in a traditional sense (e.g., medical or driver information). In particular, personally identifiable financial information includes the fact that an individual is or has been a customer of a financial institution or has obtained a financial or insurance product from it.

Information collected through the use of Internet cookies is also considered personally identifiable financial information.

Under the Act, however, nonpublic personal information does not include “publicly available information,” with that term left to be defined by regulation.

Publicly available information under the regulations means any information that a financial institution reasonably believes is lawfully made available to the general public from government records, widely distributed media, or legally required disclosures to the general public. However, an institution does not have a reasonable belief that information about a consumer is publicly available solely because that information would normally be available in public records, if the consumer has the ability in accordance with applicable law, to keep that information nonpublic. For example, an institution has a reasonable belief that an individual’s telephone number is publicly available if it has located the telephone number in the telephone book or the consumer has informed it that the telephone number is not unlisted.

<u>Privacy and Opt-Out Notices</u>

A financial institution is required to provide a clear and conspicuous notice of its privacy policies and practices to consumers before it discloses any nonpublic personal information to any nonaffiliated third party. The notice to consumers is required only if the financial institution may, in fact, share the nonpublic personal information. In addition, a financial institution must provide a privacy notice to its customers not later than when it establishes a customer relationship and at least annually thereafter. The notice to customers is required whether or not the financial institution shares nonpublic personal information. An institution may provide the initial notice to customers within a reasonable time after it establishes the customer relationship if:

(i) establishing the customer relationship is not at the customer's election;
(ii) the notice would otherwise substantially delay the customer's transaction and the customer agrees to receive the notice at a later time (e.g., a telephone transaction); or
(iii) a nonaffiliated broker-dealer or investment adviser establishes a customer relationship between the financial institution and a consumer without its prior knowledge.

Financial institutions must provide the privacy notice so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, in electronic from. Oral notices alone are insufficient. Electronic delivery should be made by e-mail (to a consumer who obtains a financial product or service electronically), or on a web page that the consumer is required to acknowledge to obtain the product or service inquires. For customers only, institutions must provide the initial notice so that it can be retained or obtained at a later time by the customer. Two or more financial institutions may provide a joint notice as long as the notice is accurate with respect to each institution. Notices may be combined with other disclosures, such as in a fund prospectus or with an annual statement.

Prior to providing nonpublic financial information to unaffiliated third parties, financial institutions must provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out. The notice must state:

(i) that the institution discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;
(ii) that the consumer has the right to opt out of that disclosure; and
(iii) a reasonable means by which the consumer may exercise the opt out right.

Institutions may require the consumer to opt out in a particular way, but it must not be too difficult; requiring the consumer to write a letter, for example, would be deemed unreasonable. Institutions must comply with a consumer's opt out direction as soon as reasonably practicable after receipt. Third parties that receive nonpublic personal information from a financial institution generally must not, directly or indirectly through an affiliate, disclose that information to any person that is not affiliated with the financial institution or the third party, unless the disclosure would be lawful if made directly by the financial institution.

In the case of consumers who are not customers, a short-form initial privacy and opt-out notice can be provided. The short-form notice must describe the opt-out right, and it must clearly and conspicuously state that the full privacy notice is available upon request.

There must be a reasonable means by which the consumer may obtain the privacy notice, such as a toll-free number or (for in-person business) requesting a copy that is immediately available.

A model privacy notice, with annotations, and a model short-form notice are attached. They can be revised as needed to meet a particular situation.

Service Providers and Joint Marketers

Financial institutions may share information with marketing and other service providers without providing consumers with an opportunity to opt out, and consumers do not thereby become customers of the service providers. However, institutions still must provide the privacy notice, and must enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the institution disclosed the information. Joint marketing and service agreements in effect as of July 1, 2000 do not have to be brought into compliance with this requirement until July l, 2002. Agreements that go into effect after July l, 2000, are subject to Regulation S-P’s general compliance date of July l, 2001, although obviously it is desirable to have them in compliance when entered into, if possible.

The notice and opt-out requirements do not apply if an institution discloses nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with;

(i) processing or servicing a financial product or service that a consumer requests or authorizes;
(ii) maintaining or servicing the consumer's account with the institution, or with another entity as a part of a private label credit card program or other extension of credit on behalf of such entity; or
(iii) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

Safeguard Procedures

Financial institutions are required to adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to:

(i) ensure the security and confidentiality of customer records and information;
(ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
(iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The actual steps to be taken to safeguard information will vary from one agency to another. It is recommended that a standard operating procedures manual describe the firm's key safeguards, which should include limiting access to customer records and information to those employees who have a legitimate business need for the information.

<u>Fair Credit Reporting Act</u>

If an entity plans to share consumer information, it must comply not only with the Gramm-Leach-Bliley Act but also with the Fair Credit Reporting Act. The Fair Credit Reporting Act generally regulates the use of "consumer reports," which it defines in section 603(d). Note that the Fair Credit Reporting Act generally does not apply to communication among affiliates, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity in advance to opt out. The Gramm-Leach-Bliley Act notice should include this disclosure.

<u>Legislative History of the Gramm-Leach-Bliley Act</u>

The Gramm-Leach-Bliley Act originally was introduced in the House of Representatives as H.R. 10, the Financial Services Act of 1999, and in the Senate as S. 900, the Financial Services Modernization Act of 1999. Neither bill as introduced included the privacy provisions that subsequently became law. The House bill was referred to the Committee on Banking and Financial Services and the Committee on Commerce, and a form of the privacy provisions was first added to the bill by the Committee on Commerce.

Although it was S.900 that was enacted into law, a number of provisions from H.R. 10, including the privacy provisions, were retained in the final statute.

The following are comments provided by the National Association of Insurance Commissioners (NAIC), in respect of their evaluation of the Act's intent and implementation:

Commissioner Kathleen Sebelius
"It's All About GLB"
NAIC/NIPR E-Regulation Conference
May 7, 2001
(as prepared)

Good morning. It's a pleasure to be with you here at the E-Regulation Conference. As you all know, there are significant transformations underway in the areas of agent licensing, rate and form filing and company licensing many of which have been brought about by the Gramm-Leach-Bliley Act. I appreciate having the chance to come here today and share with you what the NAIC members have been doing to help modernize state insurance regulation in response to these new market realities in the wake of GLB.

There's no question the marketplace is changing. New mergers and acquisitions are being reported almost daily as banks, insurance companies, and securities firms look to expand into new markets. Technology is driving every aspect of these relationships:

industry-to-industry relationships and the all important industry-to-consumer relationship. And consumers still want more products at lower costs … and they want them now.

That's the framework facing all of us … industry, consumers, *and regulators*.

As we begin this discussion, let's make clear what Congress said in Gramm-Leach-Bliley. It said — as clear as day — that states are the functional regulators of insurance. It reaffirmed the McCarran-Ferguson Act, which, as you know, recognizes the primacy and legal authority of the states to regulate all insurance activities.

In fact, I think there's a specific provision that more or less says "…no persons are permitted to engage in the business of insurance unless they are licensed by the states, as required under state law." That's quite a statement as a matter of law and Congressional intent — and it's only about 17 months old.

Gramm-Leach-Bliley

Indeed, the Gramm-Leach-Bliley Act has brought a lot of changes to the financial services industry as a whole.

But it also sent a very strong message to regulators … those of us who are *accountable* to consumers. This message extends to all regulators, not just insurance regulators. Beyond technical law requirements and directives, GLB made clear we all need to work together to make sure our regulatory systems are coordinated, efficient, and responsive to the realities of this financial services marketplace.

NAIC members are taking this message very seriously, and I am here today to tell

you a little bit about our efforts.

NAIC Is Responding To New Times, New Challenges

By now, most of you are aware of the NAIC's "Statement of Intent" … our blueprint for the modernization of state insurance regulation. An often-overlooked aspect of this initiative is the fact that it was physically signed by all commissioners representing all 50 states and the District of Columbia. That's quite a statement of our commitment to these reform initiatives.

If you gave industry advocates a blank piece of paper and asked them what kinds of reforms they wanted, they would tell you streamlined, real-time producer licensing. They'd say they want help bringing their products to market faster. They'd say they want fair and effective regulation. Well, that's what those of us elected or appointed to hold the industry accountable are doing.

And now we are putting our “Statement of Intent” pledge into action. We signed the “Statement of Intent” one year last March. Let’s take a quick look at where we are just one year later:

Responding To The Agent Licensing Requirement

- Just a year after the adoption of the NAIC’s Producer Licensing Model Act (PLMA), more than the requisite number of states are on track to meet the producer-licensing requirements of the Gramm-Leach-Bliley Act. The model creates uniformity in agent licensing procedures, simplifies the licensing process and promotes reciprocity while preserving state’s rights and eliminates retaliatory fees.
- To date, 17 states have enacted laws attempting to satisfy the GLBA reciprocity requirements.
- In addition, bills are pending in 26 states and legislative action is expected in 40 states this session.
- The National Insurance Producer Registry (NIPR) was launched to create a single point of licensing for agents to be licensed in all 50 states.
-

Implementing Privacy Protections

- After an 8-month public process, we achieved unanimous NAIC adoption of GLBA-like model privacy regulation in September 2000 that will ensure a “level playing field” for the financial services sector.

- Thirty-six states report they will enact financial privacy protections based on the GLBA/NAIC model regulation.
- Moreover, the NAIC model regulation singles out health information for additional (opt-in) protection without undermining the business of insurance.

Product Speed to Market or CARFRA (Coordinated Advertising Rate and Form Review Authority)

- On May 1, a limited launch was begun in 10 states for a single point of filing speed-to-market initiative. These states comprise 35 percent of national premium volume. More states and products will be added in 2001.
- Goals include creating greater efficiency in other filing systems, agreeing on a 30-day national review timeframe and competitive rating for commercial lines. Personal lines will also be evaluated this year.

Improvements to State-Based Systems

- We are focusing on improvements that can be made to current state-based regulatory systems for product review.
- We intend to address those product filings that will remain subject to state-based filing and review.
- Our goal is to create a more efficient state-based filing and review process that provides for consumer protection while offering uniform and consistent speed to market for insurers and consumers.

- We are developing a framework that will be used to commit states to implementing the various recommendations for efficiency that the subgroup developed.
- We are also developing a Transmittal and Review Standards Checklist, which is designed to assist state regulators in reviewing insurance product filing more efficiently and effectively.

Ensuring Cooperation between State and Federal Regulators

- The NAIC negotiated model information-sharing agreements with federal regulators. Individual states are now in the process of signing agreements with each federal regulator to facilitate the exchange of regulatory information and thus ensure better supervision and coordination.
- NAIC members are meeting regularly with federal regulators, including cross-training and education sessions.
- Members have shown increased leadership in international regulatory discussions.
- And the NAIC is now proposing new federal legislation to create regulatory efficiencies, improve dialogue and fight fraud.

Treatment of National Insurance Companies

Based on the work of the National Treatment and Coordination Working Group, we will have accomplished the following by June 2001 …

- Secured full state participation in the Uniform Certificate of Authority Application (UCAA) process.
- Developed "best practices" for a uniform company admissions process.
- Eliminated the state-specific UCAA requirements by eliminating requirements that do not add regulatory value and adding those that do add value.
- Developed an automated UCAA system.
- Developed uniform process for "corporate changes," such as adding/deleting lines of business, name changes, etc.

That's a lot of movement in just a little over a year. Many in the industry, however, were using these past 13 months to dream up a new layer of regulation and a federal bureaucracy as opposed to getting out to the state capitols to help us implement our state reforms.

It's All About Consumer Protection

Let's face the facts … Insurance is fundamentally different from banking. Figures compiled by the NAIC show that an average family could easily spend a combined total of $3,000 a year for auto, home, life, and health insurance coverage. Families with several members, more than one car, or additional property typically pay much more.

Banking, on the other hand is quite different. Show me a banking consumer who spends $3,000 on banking products because they HAVE to. Insurance, more than anything, is the sale of a promise. Consumers pay their premiums and expect to have their insurance company make good on that promise in their time of need.

Insurance is important to people. Consumers can't drive a car, buy a house or open a business without having good and affordable insurance. An NAIC member's overriding concern is protecting the consumer in all of these situations. Solvency regulation, yes, but ultimately this means taking care of your next-door neighbor, your child, or your grandma when catastrophe strikes. Or when they've been wronged.

States Have Proven Ability …

The states have 130 years of experience ensuring the solvency of insurance companies, while looking out for and protecting consumers. Having similar processes with local control is really the best of both of both worlds. Consumers need to have the confidence that the people regulating their policies have a good understanding of their local market.

In addition to that, we have a system of more than 10,000 people around the country responding to local consumer issues on a local basis every day – making sure claims get paid, answering questions, and making sure products get sold fairly. In 1999 alone, state insurance departments…

- Handled 448,000 consumer complaints
- Initiated 116,000 license cancellations, suspensions or revocations
- Suspended 113 certificates of authority

The bottom line is that there are no national consumers. Insurance is a local product that needs local regulation. It's like calling 9-1-1. When you need help, do you want that to be a local call – or one that is routed through Washington, D.C.?

Closing

In closing, I would like to say that state insurance regulation best serves its constituents by being responsive to individual consumers, being sensitive to changing markets, and encouraging insurance innovation. Those characteristics are not frequently associated with federal regulatory agencies. State regulators are in touch with what is going on within each state, and through the connection with the NAIC are also up to speed on what is happening around the country.

Together, the states are moving toward the direction of uniformity, which will make it easier for the business of insurance to be conducted across the United States. This is an effort that must first be addressed at the state level in order for the states to work together toward the most effective process for all parties affected — the insurance industry, consumers, and regulators.

It has been my great pleasure to share this information with you. It only scratches the surface of the many changes we will be facing over the next several years. I can only hope that it has been helpful to you.

As an organization of state officials responsible for protecting the public, the National Association of Insurance Commissioners is committed to maintaining a sound and non-discriminatory insurance regulatory system in the United States. With your help and support we can accomplish that goal. Remember that insurers and regulators have the same goal: Providing the insurance-buying public with the best available products at a reasonable and actuarially sound price.

The following is a summary of the new regulatory provisions:

Financial Services Modernization Act

Gramm-Leach-Bliley Act

Summary of Provisions

TITLE I -- FACILITATING AFFILIATION AMONG BANKS, SECURITIES FIRMS, AND INSURANCE COMPANIES

- Repeals the restrictions on banks affiliating with securities firms contained in sections 20 and 32 of the Glass-Steagall Act.
- Creates a new "financial holding company" under section 4 of the Bank Holding Company Act. Such holding company can engage in a statutorily provided list of

financial activities, including insurance and securities underwriting and agency activities, merchant banking and insurance company portfolio investment activities. Activities that are "complementary" to financial activities also are authorized. The nonfinancial activities of firms predominantly engaged in financial activities (at least 85% financial) are grandfathered for at least 10 years, with a possibility for a five year extension.

- The Federal Reserve may not permit a company to form a financial holding company if any of its insured depository institution subsidiaries are not well capitalized and well managed, or did not receive at least a satisfactory rating in their most recent CRA exam.

- If any insured depository institution or insured depository institution affiliate of a financial holding company received less than a satisfactory rating in its most recent CRA exam, the appropriate Federal banking agency may not approve any additional new activities or acquisitions under the authorities granted under the Act.

- Provides for State regulation of insurance, subject to a standard that no State may discriminate against persons affiliated with a bank.

- Provides that bank holding companies organized as a mutual holding companies will be regulated on terms comparable to other bank holding companies.

- Lifts some restrictions governing nonbank banks.

- Provides for a study of the use of subordinated debt to protect the financial system and deposit funds from "too big to fail" institutions and a study on the effect of financial modernization on the accessibility of small business and farm loans.

- Streamlines bank holding company supervision by clarifying the regulatory roles of the Federal Reserve as the umbrella holding company supervisor, and the State and other Federal financial regulators which ‘functionally' regulate various affiliates.

- Provides for Federal bank regulators to prescribe prudential safeguards for bank organizations engaging in new financial activities.

- Prohibits FDIC assistance to affiliates and subsidiaries of banks and thrifts.

- Allows a national bank to engage in new financial activities in a financial subsidiary, except for insurance underwriting, merchant banking, insurance company portfolio investments, real estate development and real estate investment, so long as the aggregate assets of all financial subsidiaries do not exceed 45% of the parent bank's assets or $50 billion, whichever is less. To take advantage of the new activities through a financial subsidiary, the national bank must be well capitalized and well managed. In addition, the top 100 banks are required to have an issue of outstanding subordinated debt. Merchant banking activities may be approved as a permissible activity beginning 5 years after the date of enactment of the Act.

- Ensures that appropriate anti-trust review is conducted for new financial combinations allowed under the Act.

- Provides for national treatment for foreign banks wanting to engage in the new financial activities authorized under the Act.

- Allows national banks to underwrite municipal revenue bonds

TITLE II -- FUNCTIONAL REGULATION

- Amends the Federal securities laws to incorporate functional regulation of bank securities activities.

- The broad exemptions banks have from broker-dealer regulation would be replaced by more limited exemptions designed to permit banks to continue their current activities and to develop new products.

- Provides for limited exemptions from broker-dealer registration for transactions in the following areas: trust, safekeeping, custodian, shareholder and employee benefit plans, sweep accounts, private placements (under certain conditions), and third party networking arrangements to offer brokerage services to bank customers, among others.

- Allows banks to continue to be active participants in the derivatives business for all credit and equity swaps (other than equity swaps to retail customers).

- Provides for a "jump ball" rulemaking and resolution process between the SEC and the Federal Reserve regarding new hybrid products.

- Amends the Investment Company Act to address potential conflicts of interest in the mutual fund business and amendments to the Investment Advisers Act to require banks that advise mutual funds to register as investment advisers.

TITLE III -- INSURANCE

- Provides for the functional regulation of insurance activities.

- Establishes which insurance products banks and bank subsidiaries may provide as principal.

- Prohibits national banks not currently engaged in underwriting or sale of title insurance from commencing that activity. However, sales activities by banks are permitted in States that specifically authorize such sales for State banks, but only on the same conditions. National bank subsidiaries are permitted to sell all types of insurance including title insurance. Affiliates may underwrite or sell all types of insurance including title insurance.

- State insurance and Federal regulators may seek an expedited judicial review of disputes with equalized deference.
- The Federal banking agencies are directed to establish consumer protections governing bank insurance sales.
- Preempts state laws interfering with affiliations.
- Provides for interagency consultation and confidential sharing of information between the Federal Reserve Board and State insurance regulators.
- Allows mutual insurance companies to re-domesticate.
- Allows multi-state insurance agency licensing.

TITLE IV -- UNITARY SAVINGS AND LOAN HOLDING COMPANIES

- De novo unitary thrift holding company applications received by the Office of Thrift Supervision after May 4, 1999, shall not be approved.
- Existing unitary thrift holding companies may only be sold to financial companies.

TITLE V -- PRIVACY

- Requires clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties.
- Requires a notice to consumers and an opportunity to "opt-out" of sharing of non-public personal information with nonaffiliated third parties subject to certain limited exceptions.
- Addresses a potential imbalance between the treatment of large financial services conglomerates and small banks by including an exception, subject to strict controls, for joint marketing arrangements between financial institutions.
- Clarifies that the disclosure of a financial institution's privacy policy is required to take place at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship.
- Provides for a separate rather than joint rulemaking to carry out the purposes of the subtitle; the relevant agencies are directed, however, to consult and coordinate with one another for purposes of assuring to the maximum extent possible that the regulations that each prescribes are consistent and comparable with those prescribed by the other agencies.

- Allows the functional regulators sufficient flexibility to prescribe necessary exceptions and clarifications to the prohibitions and requirements of section 502.

- Clarifies that the remedies described in section 505 are the exclusive remedies for violations of the subtitle.

- Clarifies that nothing in this title is intended to modify, limit, or supersede the operation of the Fair Credit Reporting Act.

- Extends the time period for completion of a study on financial institutions' information-sharing practices from 6 to 18 months from date of enactment.

- Provides for an effective date of 18 months after the date on which the rulemaking pursuant to section 504 is completed, to allow sufficient time for state legislatures to empower state insurance regulators to comply with this subtitle.

- Assigns authority for enforcing the subtitle's provisions to the Federal Trade Commission and the Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, according to their respective jurisdictions, and provides for enforcement of the subtitle by the States.

TITLE VI -- FEDERAL HOME LOAN BANK SYSTEM MODERNIZATION

- Banks with less than $500 million in assets may use long-term advances for loans to small businesses, small farms and small agri-businesses.

- A new, permanent capital structure for the Federal Home Loan Banks is established. Two classes of stock are authorized, redeemable on 6-months and 5-years notice. Federal Home Loan Banks must meet a 5% leverage minimum tied to total capital and a risk-based requirement tied to permanent capital

- Equalizes the stock purchase requirements for banks and thrifts.

- Voluntary membership for Federal savings associations takes effect six months after enactment.

- The current annual $300 million funding formula for the REFCORP obligations of the Federal Home Loan Banks is changed to 20% of annual net earnings.

- Governance of the Federal Home Loan Banks is decentralized from the Federal Housing Finance Board to the individual Federal Home Loan Banks. Changes include the election of chairperson and vice chairperson of each Federal Home Loan Bank by its directors rather than the Finance Board, and a statutory limit on Federal Home Loan Bank directors' compensation.

TITLE VII -- OTHER PROVISIONS

- Requires ATM operators who impose a fee for use of an ATM by a non-customer to post a notice on the machine that a fee will be charged and on the screen that a fee will be charged and the amount of the fee. This notice must be posted before the consumer is irrevocably committed to completing the transaction. A paper notice issued from the machine may be used in lieu of a posting on the screen. No surcharge may be imposed unless the notices are made and the consumer elects to proceed with the transaction. Provision is made for those older machines that are unable to provide the notices required. Requires a notice when ATM cards are issued that surcharges may be imposed by other parties when transactions are initiated from ATMs not operated by the card issuer. Exempts ATM operators from liability if properly placed notices on the machines are subsequently removed, damaged, or altered by anyone other than the ATM operator.

- Clarifies that nothing in the act repeals any provision of the CRA.

- Requires full public disclosure of all CRA agreements.

- Requires each bank and each non-bank party to a CRA agreement to make a public report each year on how the money and other resources involved in the agreement were used.

- Grants regulatory relief regarding the frequency of CRA exams to small banks and savings and loans (those with no more than $250 million in assets). Small institutions having received an outstanding rating at their most recent CRA exam shall not receive a routine CRA exam more often than once each 5 years. Small institutions having received a satisfactory rating at their most recent CRA exam shall not receive a routine CRA exam more often than once each 4 years.

- Directs the Federal Reserve Board to conduct a study of the default rates, delinquency rates, and profitability of CRA loans.

- Directs the Treasury, in consultation with the bank regulators, to study the extent to which adequate services are being provided as intended by the CRA.

- Requires a GAO study of possible revisions to S corporation rules that may be helpful to small banks.

- Requires Federal banking regulators to use plain language in their rules published after January 1, 2000.

- Allows Federal savings associations converting to national or State bank charters to retain the term "Federal" in their names.

- Allows one or more thrifts to own a banker's bank.

- Provides for technical assistance to miccroenterprises (meaning businesses with fewer than 5 employees that lack access to conventional loans, equity, or other banking services). This program will be administered by the Small Business Administration.

- Requires annual independent audits of the financial statements of each Federal Reserve bank and the Board of Governors of the Federal Reserve System.

- Authorizes information sharing among the Federal Reserve Board and Federal or State authorities.

- Requires a GAO study analyzing the conflict of interest faced by the Board of Governors of the Federal Reserve System between its role as a primary regulator of the banking industry and its role as a vendor of services to the banking and financial services industry.

- Requires the Federal banking agencies to conduct a study of banking regulations regarding the delivery of financial services, and recommendations on adapting those rules to online banking and lending activities.

- Protects FDIC resources by restricting claims for the return of assets transferred from a holding company to an insolvent subsidiary bank.

- Provides relief to out-of-State banks generally by allowing them to charge interest rates in certain host states that are no higher than rates in their home states.

- Allows foreign banks generally to establish and operate Federal branches or agencies with the approval of the Federal Reserve Board and the appropriate banking regulator if the branch has been in operation since September 29, 1994 or the applicable period under appropriate State law.

- Expresses the sense of the Congress that individuals offering financial advice and products should offer such services and products in a nondiscriminatory, nongender-specific manner.

- Permits the Chairman of the Federal Reserve Board and the Chairman of the Securities and Exchange Commission to substitute designees to serve on the Emergency Oil and Gas Guarantee Loan Guarantee Board and the Emergency Steel Loan Guarantee Board.

- Repeals section 11(m) of the Federal Reserve Act, removing the stock collateral restriction on the amount of a loan made by a State bank member of the Federal Reserve System.

- Allows the FDIC to reverse an accounting entry designating about $1 billion of SAIF dollars to a SAIF special reserve, which would not otherwise be available to the FDIC unless the SAIF designated reserve ratio declines by about 50% and would be expected to remain at that level for more than one year.

- Allow directors serving on the boards of public utility companies to also serve on the boards of banks.

These provisions have, therefore, placed requirements on financial institutions to

provides privacy notices. The following is a model example of two such notices:

MODEL PRIVACY NOTICE WITH ANNOTATIONS

1. Give a general description of the purpose of the notice:

Your Privacy Is Important to Us

We are committed to maintaining the confidentiality, integrity and security of your personal information. When you provide personal information, we believe that you should be aware of our policies to protect the confidentiality of that information.

2. Describe the categories of nonpublic personal information that you collect. Here and elsewhere, omit the references to "our affiliates" if you have no affiliates:

In order to ensure we are able to offer and provide you with the most appropriate services, we collect nonpublic personal information about you from the following sources:

- ***Information we receive from you on applications or other forms***;
- ***Information about your transactions with us, our affiliates, or others; and***
- ***Information we receive from a consumer-reporting agency.***

3. If you do not share nonpublic personal information with anyone, (except for servicing and processing transactions and except for certain legal exceptions), you can say so, then skip to #8. The exceptions for servicing and processing transactions are described in section 248.14 of the SEC's Regulation S-P (or comparable provisions of other regulations) and the legal exceptions are described in section 248.15 of Regulation S-P (or comparable provisions of other regulations).

We do not disclose any nonpublic personal information about out customers or former customers to anyone except as permitted by law.

4A. If you do share nonpublic personal information or wish to reserve the right to do so, describe the categories of nonpublic personal information that you may share. Here is one example (which you should alter as necessary), or you can use the alternative language in #4B, below. Do not discuss your arrangements with service providers and joint marketers here; describe those arrangements below in #7A or #7B.

Further, in order to provide better service to you, or to keep you advised of products and services that we think may be useful to you, we may, from time to time, disclose the following kinds of nonpublic personal information about you:

- **Information we receive from you on applications and other forms, such as your name, address, social security number, assets, and income;**

- **Information about your transactions with us and/or our affiliates[11] or others, such as your account size, payment history, and history with our Company; and**

- **Information we receive from a consumer-reporting agency, such as your creditworthiness and credit history.**

4B. Instead of the more specific description in #4A, you can simply say that you may share all of the information you collect.

Further, in order to provide better service to you, or to keep you advised of products and services that we think may be useful to you, we may, from time to time, disclose all of the information that we collect, as described above.

[11] Remember to use reference to "affiliates" only if relevant to your Company.

5. Describe the affiliates and nonaffiliated third parties with whom you may share nonpublic personal information. Feel free to change specific references as warranted by your operations. You can be specific, or you can use the format below:

We may disclose nonpublic personal information about you to the following types of third parties:

- **Our affiliates, which include (name or briefly describe);**
- **Financial services providers, such as mortgage bankers, securities broker-dealers, and other insurance brokers or agents;**
- **Non-financial companies, such as retailers, direct marketers, airlines, and publishers; and**
- **Others, such as non-profit organizations.**

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

6. Describe the categories of nonpublic personal information about your former customers that you share and the categories of affiliates and nonaffiliated third parties with whom it is shared. The format below assumes that you do not have any special treatment for former customers.

We may disclose nonpublic personal information about our former customers to the same extent as for our current customers.

7A. If you share nonpublic personal information with service providers and joint marketers under contact with you, describe the categories of information you share and the categories of third parties with whom you have contracted. (Note that these arrangements must comply with section 248.13 of Regulation S-P, or comparable provisions of other regulations.) Here is one example (which you should alter as necessary), or you instead can use the alternative language in #7B.

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- **Information we receive from you on applications or other forms, such as your name, address, social security number, assets, and income;**

- **Information about your transactions with us and/or our affiliates[12] or others, such as your account size, payment history, and history with our Company;**

- **Information we receive from a consumer-reporting agency, such as your creditworthiness and credit history.**

7B. Instead of the more specific description in 7#A, you can simply say that you may share all of the information you collect with joint marketers (or other service providers).

We may disclose all of the information we collect, as described above, to companies that perform marketing services on our behalf or to other financial institutions, insurance companies, agents, brokers, retailers and wholesalers or other industry vendors with whom we have joint marketing agreements.

8. If you wish, you may include a reservation of your rights to share additional information in the future.

[12] See footnote 1.

We reserve the right to disclose all of the information that we collect, as described above, to any affiliates that we may have at the time[13] and to the following types of third parties:

- **Financial service providers, such as mortgage bankers, and insurance companies, agents, brokers, retailers, and wholesalers;**

- **Non-financial companies, such as retailers, direct marketers, airlines, and publishers; and**

- **Others, such as non-profit organizations.**

9. If you share information with your affiliates[14] (other than identifying information and information as to your transactions or experiences with the consumer), disclose that the information may be shared and that the consumer has the opportunity to direct that it not be shared. Use the same opt-out method as in #10, below.

The law permits us to share certain kinds of information with our affiliates, including identifying information and information about your transactions with us. We may also share other information with our affiliates, including information we receive from you on applications and other forms, and information we receive from a consumer-reporting agency. If you prefer that we not share these kinds of information with our affiliates, you may direct us not to

---

[13] See footnote 1.
[14] See footnote 1.

share this information by calling us at the following toll-free number: (insert number), or by sending us a letter to this effect addressed to: (insert name of responsible person and address).

In this respect, it is advisable to establish a protocol by which to acknowledge, in writing, receipt of the consumer's request in order to document their directives. Maintain a record of all telephone calls and letters in a separate log and file.

10. If you share nonpublic personal information with nonaffiliated third parties (other than service providers and joint marketers, servicing and processing transactions, and certain legal exceptions – see #3 and #7A, describe the consumer's right to opt out. The opportunity to opt out must be reasonable, such as by mailing a form or calling a toll-free telephone number.

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures; that is, you may direct us not to make those disclosures (other than those disclosures permitted by law). If you prefer that we not share these kinds of information with nonaffiliated third parties, you may elect to opt-out of the disclosures and direct us not to do so by calling the following toll-free number: (insert number), or by sending us a letter to this effect addressed to: (insert name of responsible person and address).

Again, and in this respect, it is advisable to establish a protocol by which to acknowledge, in writing, receipt of the consumer's request in order to document their directives. Maintain a record of all telephone calls and letters in a separate log and file.

11. Briefly describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

We restrict access to nonpublic personal information about you to those employees with a legitimate business need for the information. We maintain physical, electronic and procedural safeguards that comply with federal standards to guard and protect your nonpublic personal information.

Thank you for your assistance and cooperation. Our only goal is to ensure we provide the best products and services to you, and that we comply with all federal and state laws applicable to you and your business. Please feel free to contact us in the event you should have any questions or need further information.

SHORT – FORM NOTICE

You can also provide consumers who are not customers this short-form notice, instead of giving your full privacy notice. This document contains model short-form notice language, with annotations in bold Italics.

Important Privacy Notice

1. If you share information with your affiliates[15] (other than identifying information and information as to your transactions or experiences with the consumer),

[15] See footnote 1.

disclose that the information may be shared and that the consumer has the opportunity to direct that it not be shared.

The law permits us to share certain kinds of information with our affiliates, including identifying information and information about your transactions with us. We may also share other information with our affiliates, including information we receive from you on applications and other forms, and information we receive from a consumer-reporting agency. If you prefer that we not share these kinds of information with our affiliates, you may direct us not to do so by calling the following toll-free number: (insert number), or by sending us a letter to this effect addressed to: (insert name of responsible person and address).

2. If you disclose nonpublic personal information (beyond the disclosures permitted by sections 248.13, 248.14 and 248.15 of Regulation S-P, or comparable provisions of other regulations), describe the right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties. The consumer's opportunity to opt out must be reasonable, such as by mailing a form or calling a toll-free number.

We may disclose nonpublic personal information about you to nonaffiliated third parties. If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of these disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of the disclosures to nonaffiliated third parties, you may call the following

toll-free number: (*insert number*), or by sending us a letter to this effect addressed to: (insert name of responsible person and address).

3. Tell the consumer how to obtain a copy of your full privacy notice. Normally this will be by calling a toll-free telephone number or, for a consumer who conducts business in person at your office, by requesting a copy that you will immediately provide.

A copy of our full privacy notice is available upon request. To obtain it, you may call the following toll-free telephone number: (*insert number*) or, send us a letter with your request addressed to: (insert name of responsible person and address).

4. Briefly describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

We restrict access to nonpublic personal information about you to those employees with a legitimate business need for the information. We maintain physical, electronic and procedural safeguards that comply with federal standards to guard and protect your nonpublic personal information.

Thank you for your assistance and cooperation. Our only goal is to ensure we provide the best products and services to you, and that we comply with all federal and state laws applicable to you and your business. Please feel free to contact us in the event you should have any questions or need further information.

RETAILER'S GENERAL STATEMENT

Letterhead of Retailer

Date: _______________

Compliance Statement

This will confirm we have issued a Privacy Notice to all prospective/named insureds whose information; materials and supporting documentation will be attached to submissions we will be providing for consideration as of July 1, 2001. The privacy notices were issued pursuant to the provisions of the Gramm-Leach-Bliley/Financial Modernization Act regarding the collection, use and disclosure of non-public personal information of the prospective/named insured.

Unless otherwise noted or advised, this will further confirm that we have not received instructions from the prospective/named insured that the non-public personal information conveyed or collected not be disclosed to third parties.

We are in compliance with all provisions of the Gramm-Leach-Bliley/Financial Modernization Act, and have the requisite and appropriate procedures in place within our agency to protect the privacy of non-public personal information of our consumers and customers who elect not to have such information disclosed or shared.

Gramm Leach Bliley Conference Report Summary

TITLE III - INSURANCE

SUBTITLE A - STATE REGULATION OF INSURANCE

Senate Position: The Senate bill contains a number of provisions intended to preserve State regulation of insurance.

House Position: The House amendment similarly contains a number of provisions intended to preserve and enhance State regulation of insurance.

Conference Substitute: The Senate receded to the House with an amendment.
In general, Subtitle A of Title III reaffirms that States are the regulators for the insurance activities for all persons, including acting as the functional regulator for the insurance activities of federally chartered banks. This functional regulatory power is subject to section 104 of Title I, however, which sets forth the appropriate balance of protections against discriminatory actions. Federally chartered banks and their subsidiaries are prohibited from underwriting insurance, except for authorized products. A rule of construction was added by the Conference Committee to prevent evasion of State insurance regulation by foreign reinsurance subsidiaries or offices of domestic banks, clarifying that providing insurance (including reinsurance) outside of the United States to indemnify an insurance product or company in a State shall be considered to be providing insurance as principal in that State.

Federally chartered banks are prohibited from engaging in any activity involving the underwriting or sale of title insurance, except that national banks may sell title insurance products in any State in which state-chartered banks are authorized to do so (other than through a "wild card provision"), so long as such sales are undertaken "in the same manner, to the same extent, and under the same restrictions" that apply to such state-chartered banks. Certain currently and lawfully conducted title insurance activities of banks are grandfathered, and existing State laws prohibiting all persons from providing title insurance are protected.

An expedited and equalized dispute resolution mechanism is established to guide the courts in deciding conflicts between Federal and State regulators regarding insurance issues. The "without unequal deference" standard of review does not apply to State regulation of insurance agency activities that were issued before September 3, 1998 (other than those protected by the scope of the safe harbor provision of section 104).
The Federal banking agencies are required to issue final consumer protection regulations within one year, to provide additional safeguards for the sale of insurance by any bank or other depository institution, or by any person at or on behalf of such institution.
State laws that prevent or significantly interfere with the ability of insurers to affiliate, become an FHC, or demutualize, are preempted, except as provided in section 104(c)(2), and with respect to demutualizing insurers for the State of domicile (and as set forth in the Redomestication Subtitle). State laws limiting the investment of an insurer's assets in a depository institution are also preempted, except that an insurer's State of domicile may limit such investment as provided.

The Federal banking agencies and the State insurance regulators are directed to coordinate efforts to supervise companies that control both depository institutions and persons engaged in the business of insurance, and to share, on a confidential basis, supervisory information including financial health and business unit transactions. The agencies are further directed to provide notice and to consult with the State regulators before taking actions which effect any affiliates engaging in insurance activities. A banking regulator is not required to provide confidential information to a State insurance regulator unless such State regulator agrees to keep the information in confidence and make all reasonable efforts to oppose disclosure of such information. Conversely, Federal banking regulators are directed to treat as confidential any information received from a State regulator which is entitled to confidential treatment under State law, and to make similar reasonable efforts to oppose disclosure of the information.

SUBTITLE B - REDOMESTICATION OF MUTUAL INSURERS

Senate Position: No provision.

House Position: The House bill allows mutual insurance companies to redomesticate to another state and reorganize into a mutual holding company or stock company. It only applies to insurers in States which have not established reasonable terms and conditions for allowing mutual insurance companies to reorganize into a mutual holding company. All licenses of the insurer are preserved, and all outstanding policies, contracts, and forms remain in full force. A redomesticating company must provide notice to the state insurance regulators of each State for which the company is licensed. A mutual insurance company may only redomesticate under this Subtitle if the State insurance regulator of the new (transferee) domicile affirmatively determines that the company's reorganization plan meets certain reasonable terms and conditions: the reorganization is approved by a majority of the company's board of directors and voting policyholders, after notice and disclosure of the reorganization and its effects on policyholder contractual rights; the policyholders have equivalent voting rights in the new mutual holding company as compared to the original mutual insurer; any initial public offering of stock shall be in accordance with applicable securities laws and under the supervision of the State insurance regulator of the transferee domicile; the new mutual holding company may not award any stock options or grants to its elected officers or directors for six months; all contractual rights of the policyholders are preserved; and the reorganization is approved as fair and equitable to the policyholders by the insurance regulators of transferee domicile.

Conference Substitute: The Senate receded to the House with an amendment.

SUBTITLE C - NATIONAL ASSOCIATION OF REGISTERED AGENTS AND BROKERS

Senate Position: The Senate bill contains a sense of the Congress statement that States should provide for a uniform insurance agent and broker licensing system.

House Position: The House bill encourages the States to establish uniform or reciprocal requirements for the licensing of insurance agents. If a majority of the States do not establish uniform or reciprocal licensing provisions within a three-year period (as determined by the National Association of Insurance Commissioners ["NAIC"]), then the National Association of Registered Agents and Brokers ("NARAB") would be established as a private, non-profit entity managed and supervised by the State insurance regulators. State insurance laws and regulations shall not be affected except to the extent that they are inconsistent with a specific requirement of the Subtitle. Membership in NARAB is voluntary and does not affect the rights of a producer under each individual state license. Any state-licensed insurance producer whose license has not been suspended or revoked is eligible to join NARAB. NARAB shall be base membership criteria on the highest levels insurance producer qualification set by the States on standards such as integrity, personal qualification, education, training, and experience. NARAB members shall continue to pay the appropriate fees required by each State in which they are licensed, and shall renew their membership annually. NARAB may inspect members records, and revoke a membership where appropriate. NARAB shall establish an Office of Consumer Complaints, which shall have a toll-free phone number (and Internet website) to receive and investigate consumer complaints and recommend disciplinary actions. The Office shall maintain records of such complaints, which shall be made available to the NAIC and individual State insurance regulators, and shall refer complaints where appropriate to such regulators.

If the NAIC determines that the States have not met the uniformity or reciprocity requirements, then the NAIC has two years to establish NARAB. The NAIC shall appoint NARAB's board of directors, some of whom must have significant experience with the regulation of commercial insurance lines in the 20 States with the most commercial lines business. If within the time period allotted for NARAB's creation, the NAIC has still not appointed the initial board of directors for NARAB, then the initial directors shall be the State insurance regulators of the seven States with the greatest amount of commercial lines insurance. NARAB's bylaws are required to be filed with the NAIC, taking effect 30 days after filing unless disapproves by the NAIC as being contrary to the public interest or requiring a public hearing. The NAIC may require NARAB to adopt or repeal additional bylaws or rules as it determines appropriate to the public interest. The NAIC is given the responsibility of overseeing NARAB, and is authorized to examine and inspect NARAB's records, and require NARAB to furnish it with any reports.

If at the end of two years after NARAB is required to be established, (1) a majority of the States representing at least 50% of the total commercial-lines insurance premiums in the United States have not established uniform or reciprocal licensing regulations, or (2) the NAIC has not approved NARAB's bylaws or is unable to operate or supervise NARAB (or if NARAB is not conducting its activities under this Act), then NARAB shall be created and supervised by the President, and shall exist without NAIC oversight. The President shall appoint NARAB's board, with the advice and consent of the Senate, from lists of candidates submitted by the NAIC. If the President determines that NARAB's board is not acting in the public interest, the President may replace the entire board with new members (subject to the advice and consent of the Senate). The President may also suspend the effectiveness of any rule or action by NARAB which the

President determines is contrary to the public interest. NARAB shall report annually to the President and Congress on its activities.

State laws regulating insurance licensing that discriminate against NARAB members based on non-residency are preempted, as well as State laws and regulations which impose additional licensing requirements on non-resident NARAB members beyond those established by the NARAB board (pursuant to this Subtitle), except that State unfair trade practices and consumer protection laws are protected from preemption, including counter-signature requirements. NARAB is required to coordinate its multistate licensing with the various States. It is also required to coordinate with the States on establishing a central clearinghouse for license issuance and renewal, and for the collection of regulatory information on insurance producer activities. NARAB shall further coordinate with the NASD to facilitate joint membership. Any dispute involving NARAB shall be brought in the appropriate U.S. District Court under federal law, after all administrative remedies through NARAB and the NAIC have been exhausted.

Conference Substitute: The Senate receded to the House.

SUBTITLE D - RENTAL CAR AGENCY INSURANCE ACTIVITIES

Senate Position: The Senate bill provides that the requirements under section 104 with respect to mandatory licensing do not apply to persons who offer insurance connected with a short term motor vehicle rental so long as the State does not require such licensing.

House Position: The House bill creates a Federal presumption for a three-year period that no State law imposes any licensing, appointment, or education requirements on persons who rent motor vehicles for a period of 90 days or less and sell insurance to customers in connection with the rental transaction. This presumption shall not apply to a State statute, the prospective application of a statutorily-authorized final State regulation or order interpreting a State statute, or the prospective application of a court judgment interpreting or applying a State statute, if such State statute or final State regulation or order specifically and expressly regulates (or exempts from regulation) persons who solicit or sell such short term vehicle rental insurance. This presumption shall apply to the retroactive application of a final State regulation or order interpreting a general State insurance licensing statute, or the retroactive application of a court judgment interpreting or applying a general State insurance licensing statute, with respect to the regulation of persons who solicit or sell such short term vehicle rental insurance.

Conference Substitute: The Senate receded to the House.

SUBTITLE E – CONFIDENTIALITY

Senate Position: No provision.

House Position: The House bill requires insurance companies and their affiliates to protect the confidentiality of individually identifiable customer health and medical and genetic information. Such companies may only disclose such information with the consent of the customer or for statutorily specified purposes.

Conference Substitute: The House receded to the Senate

Gramm Leach Bliley Conference Report Summary

TITLE V - PRIVACY

SUBTITLE A - DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION

Senate Position: No provision.

House Position: The House bill contained important provisions providing consumers with new protections with respect to the transfer and use of their nonpublic personal information by financial institutions.

Among other things, the House bill directed relevant regulators to establish comprehensive standards for ensuring the security and confidentiality of consumers' personal information maintained by financial institutions; allowed customers of financial institutions to "opt out" of having their personal financial information shared with nonaffiliated third parties, subject to certain exceptions; barred financial institutions from disclosing customer account numbers or similar forms of access codes to nonaffiliated third parties for telemarketing or other direct marketing purposes; and mandated annual disclosure - in clear and conspicuous terms - of a financial institution's policies and procedures for protecting customers' nonpublic personal information.

Conference Substitute: The Senate receded to the House with an amendment.
The amendment modified the House position in the following ways:

1. The Federal functional regulators, the Secretary of the Treasury, and the FTC, in consultation with State insurance authorities, are directed to prescribe such regulations as may be necessary to carry out the purposes of the privacy subtitle. The House bill had called for a joint rulemaking. The relevant agencies are required to consult and coordinate with one another in order to assure to the maximum extent possible that the regulations each prescribes are consistent and comparable with those prescribed by the other agencies. It is the hope of the Conferees that State insurance authorities would implement regulations necessary to carry out the purposes of this title and enforce such regulations as provided in this title.

2. To address the concern that the House bill failed to provide a mechanism for enforcing the subtitle's provisions against non-financial institutions, the Conferees agreed to clarify that the FTC's enforcement authority extends to such entities.

3. The Conferees agreed to clarify the relation between Title V's privacy provisions and other consumer protections already in law, by stating that nothing in the title shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act, and no inference shall be drawn on the basis of the provisions of the title regarding whether information is transaction or experience information under section 603 of that Act.

4. At the request of the Conferees from the Committee on Agriculture, the Conferees agreed to exclude from the scope of the privacy title any person or entity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act, as well as the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971. The Conferees also excluded from this subtitle institutions chartered by Congress specifically to engage in securitization or secondary market transactions, so long as such institutions do not sell or transfer nonpublic personal information to nonaffiliated third parties. The Conferees granted the exception based on the understanding that the covered entities do not market products directly to consumers.

5. The Conferees agreed to clarify that a financial institution's annual disclosure of its privacy policy to its customers must include a statement of the institution's policies and practices regarding the sharing of nonpublic personal information with affiliated entities, as well as with nonaffiliated third parties.

6. The Conferees agreed to provide that the disclosure of nonpublic personal information contained in a consumer report reported by a consumer reporting agency does not fall within section 502's notice and opt out requirements.

7. The Conferees agreed to modify the statutory definition of "nonpublic personal information" by clarifying that such term does not encompass any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

8. The Conferees agreed to exclude disclosures to consumer reporting agencies from section 502(d)'s limitations on the sharing of account number information.

9. The Conferees agreed to give the relevant regulatory agencies the authority to prescribe exceptions to subsections (a) through (d) of section 502, rather than just sections 502(a) and (b), as provided for in the House bill.

10. The Conferees inserted language stating that the privacy provisions in the subtitle do not supersede any State statutes, regulations, orders, or interpretations, except to the

extent that such State provisions are inconsistent with the provisions of the subtitle, and then only to the extent of the inconsistency. The amendment provides that a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subtitle if the protection such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this subtitle, as determined by the FTC in consultation with the agency or authority with jurisdiction under section 505(a) over either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.

11. Section 506 authorizes the Federal banking agencies and the National Credit Union Administration to prescribe joint regulations governing the institutions under their jurisdiction with respect to the Fair Credit Reporting Act; the Conferees agreed to an

amendment giving the Board of Governors of the Federal Reserve the authority to prescribe FCRA regulations governing bank holding companies and their affiliates.

12. The Conferees agreed to modify section 502(e)(5), to include the Secretary of the Treasury as a "law enforcement agency" for the purposes of the Bank Secrecy Act, to avoid unintended interference with the existing functions of the Treasury's anti-money laundering unit, the Financial Crimes Enforcement Network ("FinCEN").

The Conferees wish to ensure that smaller financial institutions are not placed at a competitive disadvantage by a statutory regime that permits certain information to be shared freely within an affiliate structure while limiting the ability to share that same information with nonaffiliated third parties. Accordingly, in prescribing regulations pursuant to this subtitle, the agencies and authorities described in section 504(a)(1) should take into consideration any adverse competitive effects upon small commercial banks, thrifts, and credit unions. In issuing regulations under section 503, the regulators should take into account the degree of consumer access to disclosure by electronic means. In exercising their authority under section 504(b), the agencies and authorities described in section 504(a)(1) may consider it consistent with the purposes of this subtitle to permit the disclosure of customer account numbers or similar forms of access numbers or access codes in an encrypted, scrambled, or similarly coded form, where the disclosure is expressly authorized by the customer and is necessary to service or process a transaction expressly requested or authorized by the customer.

The Conferees recognize the need to foster technological innovation in the financial services and related industries. The Conferees believe that the development of new technologies that facilitate consumers' access to the broad range of products and services available through online media should be encouraged, provided that such technologies continue to incorporate safeguards for consumer privacy.

SUBTITLE B - FRAUDULENT ACCESS TO FINANCIAL INFORMATION

Senate Position: The Senate bill contained provisions making it a Federal crime - punishable by up to five years in prison - to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed, customer information of a financial institution through fraudulent or deceptive means, such as by misrepresenting the identity of the person requesting the information or otherwise misleading an institution or customer into making unwitting disclosures of such information. In addition, it provided for a private right of action and enforcement by state attorneys general.

House Position: Similar provisions, with no private right of action or enforcement by State Attorneys General.

Conference Substitute: The Senate receded to the House with an amendment.
The amendment provided that authority for enforcing the subtitle would be placed in the FTC, the Federal banking agencies and the National Credit Union Administration (for enforcement of these provisions with respect to compliance by depository institutions within their jurisdiction).

Technology

With Y2K safely behind us, the major concerns in this area involve software and, of course, electronic commerce. The indispensability of computers to the functioning of nearly every institution, commercial and not, means that when computers don't function for whatever reason, or don't meet the expectations of a user, there will be lawsuits. Many of these suits will be standard breach of contract claims that will likely not be covered by insurance. However, they may also trigger errors and omissions policies. A number of insurers are putting together defense and coverage panels specifically equipped to deal with technology claims and the issues they raise.

Intellectual property

This is a natural segue from technology. And it's actually a very interesting and significant area. The exposures created in this area are quite significant and the coverage issues turn established notions of insurance coverage on their head. We will address three things.

- First, the nature of the coverage that's involved.
- Second, the dovetailing of the broad coverage with the sweeping changes that are occurring in our society's methods of doing business.
- Third, and finally, the financial implications of these claims.

Let's begin by reviewing the provisions of the typical advertising injury coverage part.

> "We will pay for damages because of advertising injury for which the laws hold anyone we protect responsible and which are covered by your policy. We cover only advertising injury caused by an offense committed during the policy period and in the course of advertising your goods, products, or services. . . ."

So to recap, two elements are required: (1) advertising injury (2) in the course of advertising. What is advertising injury? It can constitute:

- slander, libel or disparagement
- violation of a right of privacy
- misappropriation of advertising ideas or style of doing business

– infringement of copyright, title, or slogan

There are very few operative exclusions. Simply the following:

– -no coverage for willful violation of a penal statute

– -no coverage for a publication that first occurred before the effective date of the policy

– -no coverage for publication of material known to be false.

There is typically no limitation to non-intentional conduct.

Consider also some of the sorts of things that may be covered under the advertising injury coverage part:

A husband takes hidden video pictures of the family au pair girl taking a shower and sells them on the Internet. He sells them, in part by showing a couple of frames of the videos. This scenario – from an actual case – is an advertising injury (that is, an invasion of privacy).

Here's another example. A small business decides to make cookie stamps. These are ceramic stamps that impress designs on cookies - like geese and Christmas wreathes –

which are to be sold in craft shops and gourmet stores. There's another business that's already making these items, and what the small business does is to buy some of the other's stamps, and to get hold of its catalog. Before long, the small business is turning out the same cookie stamps - even a duplicate catalog. The other business sues for misappropriation of its style of doing business. And the small business demands coverage. Would this be held a covered claim? The plaintiff in that case received a verdict of almost $12 million.

In the technology sector, perhaps the biggest intellectual property war being waged right now is over the use of "metatags." Basically, a metatag is an invisible field within a web site containing certain key words or descriptors that pertain to the content of the site. An insurance company's web site, for example, would probably have a metatag that includes words such as insurance, coverage, insurer, etc. Consequently, when a web user, not sure of that company's internet address, visits a search engine and types the term "insurance," he will receive that company's web page as a "hit." This is all fine and well until one party uses a trademark owned by another party in a metatag, so as to siphon business away from the other.

A famous example of this occurred in the "Moviebuff" case. In that case, the US Court of Appeals for the Ninth Circuit was faced with a suit in which the defendant had used the plaintiff's trademark "moviebuff" in its metatags, so that when an internet user visited a search engine site such as Lycos and entered moviebuff as a search query, the defendant's competing web site would appear as a match. The court found that consumers looking for the plaintiff's products might be initially confused when the use of "moviebuff" as a search term brought them to the defendant's web site. It therefore prohibited the use of the term in the defendant's metatags. The injury, if any, done here would qualify as an advertising injury.

When it comes to intellectual property and advertising injury, there is presently no help from our courts. They seem to be getting hung up on what constitutes advertising. Since that term, unlike "advertising injury," is not defined, some judges are ignoring it entirely. Some are deciding that pretty much any kind of business activity is, in effect, advertising. Still others are deciding it is ambiguous, with its definition and interpretation to be construed against the drafter. Consider for a moment what it means if the advertising element is disregarded. Then any invasion of privacy could be covered, as could any trade disparagement.

We may be only beginning to see the potential for claims under this coverage part. Our ways of doing business are changing at a pace faster than at any time since the early Renaissance. You cannot find a period in history like this unless you go back five hundred years to the invention of the printing press and the discovery of the new world.

We now live in a world of hyperlinks, domain names, servers, segues, e-commerce, and so forth. Which one of these concepts is a style of doing business? Maybe all of them.

Last but not least, there is, of course, the financial dimension. These might well be called the "bet the company" claims. It's where one start-up business sues another, with each claiming that it was headed straight for the top – like another Amazon.com. The damages figures that one sees in these cases are astronomical. In fact, there are few claims of e-commerce advertising injury that are not a policy limits case. That makes them especially hard to settle, and extremely expensive to defend. And consider this: because of the terrifying exposure they present to the insured, they can present extracontractual claims in waiting.

In the *Surgin Surgical Instruments* case in California a few years ago, judgment was entered for the plaintiff policyholder and against the insurer for failure to defend a patent infringement suit. Compensatory damages were $572,549; and punitive damages were $57,200,000. The judgment was overturned on appeal, but it was enough to make many sit up and take notice of the quality of defense which must be afforded, the budgetary dollars needed to defend them to the final curtain, and the education process necessary to ensure judges and juries enter the proper verdicts.

Financial Services Consolidation

The privacy issues in the areas of technology and advertising have already been addressed. However, there are more. Suppose a person applies for a loan at the local bank and the bank determines that the interest rate that should be paid on the loan is a great deal higher than the rate that of a co-worker on a similar loan. When the difference is discovered, additional information on this discrepancy is requested. The applicant is advised the interest rate is higher because of his heart condition. The loan application submitted is devoid of any such information.

As it turns out, the heart condition was not revealed to the loan officer or even to the bank, but was disclosed years ago on an application for health insurance. The insurance company is now owned by the applicant's bank.

Does a claim exist against the insurance company for invasion of privacy? Or against the bank for discrimination? With some creativity, it may be possible. With the recent enactment of the Financial Services Modernization Act, the old barriers between the securities, banking and insurance industries have been removed. So now insurance companies can own banks and banks can operate securities companies, and all of them can share customer information with each other and with the other companies with which they do business.

Emloyment Practices

The principal developments in the area of sexual harassment and other sex related claims have come in the employment context and in connection with claims against public entities. More than 450 employment suits are filed in the U.S. everyday. Fifty-six percent of all employment cases that are tried result in a verdict for the plaintiff, and the average verdict exceeds $250,000. 15% of the verdicts are over $1 million. The largest numbers of these claims are filed in Texas, California, Florida and Illinois. These claims are not all about sex, but many are.

Not long ago, employees who were sexually harassed by their boss had little recourse, especially if they could not prove that their careers were damaged by the conduct. Recent Supreme Court decisions regarding sexual harassment in the workplace, however, now make it easier for employees to sue not just their harasser but also an employer who failed to adequately address the problem. In opinions rendered in the past several years, the high court held that employers can be vicariously liable for sexual harassment by a supervisor even if the victim suffers no negative job consequences.

But more than just businesses, public entities are also under fire. For example, in Cook County, Illinois, a recent sexual harassment case cost the county over $400,000 in defense costs alone. The Supreme Court recently held that in some circumstances, a private Title 9 damages action may lie against a school board in cases where a student is harassed.

And now, sexual harassment claims are beginning to be seen in a new area: the .com companies. These companies pride themselves on creating the “ultimate anti-corporate environment.” This mentality, combined with the fact that the priority is often just remaining afloat in the early days, spurs a no-holds-barred, almost wild corporate culture. Less rules and policies. Not only that, but the long hours, and close working quarters can breed workplace relationships that ultimately can turn into sexual harassment claims.

But how does all of this affect insurance companies? Traditionally it has been thought that such claims are not covered under CGL policies because the conduct on the part of the harasser would be considered intentional. However, plaintiff lawyers are getting smarter, and they are pleading their complaints more carefully. Sexual harassment claims are being described as defamation claims, discrimination claims and invasion of privacy claims. And of course, many policies now cover such claims via the Personal Injury coverage part, which is part of the Advertising Injury part we discussed before. Also, Employment Practices Liability Coverage (known as EPLI policies, for short) provide coverage for these types of claims by design.

Under these policies, the insurer agrees to pay loss from claims made against the insured persons during the policy period for wrongful acts, including “employment practices wrongful acts." And an "employment practices wrongful act" is defined, in part, to mean "discrimination or sexual harassment adversely affecting any employee of, or applicant for employment with, the insured company." So, whether or not Underwriters specifically provide cover for sexual harassment claims, or have outward reinsurance cover that does, the fact remains that the issue is an important one.

Drugs

Drug claims are serious and potentially very expensive for any carrier with insureds in the biotech, drug manufacturing, or health-care industries. On the heels of fen-phen and its compatriots has come another problem drug: Rezulin, a product made by Warner-Lambert to treat Type II diabetes. Just recently, a class action was filed in federal court on behalf of one million plaintiffs against Warner Lambert to pay for medical monitoring, with claimants claiming the drug causes liver damage.

Experts are comparing the potential magnitude of the injuries caused by Rezulin to the magnitude of the injuries caused by the diet drugs which headlined a US$4.8 billion class action. As competition among global drug manufacturers and the ROI increase, the opportunity that more potential claims will emerge from these products remains fairly significant.

Environmental Enforcement

No emerging claims discussion would be complete without some reference to environmental claims. As noted at the outset, emerging claims follow our country's developing and emerging industries, and environmental claims clearly followed our industrial development. That does not mean, however, that the problem has retreated or gone away. They just have not been making headlines for a while. In fact, there is a one trillion dollar Superfund bill that remains to be paid. The current administration's enforcement efforts may well place political priority on cleanup enforcement, with the consequence of the "potentially responsible parties" looking to their insurers for cover.

In fact, many states are currently in the process of passing laws that allow compensation to policyholders under their CGL policies for environmental clean-up and litigation costs. This, of course, only really implicates policies written before 1970 because they did not include pollution exclusions. In these states, the high courts are holding that "gradual pollution" qualifies as "sudden and accidental" damage which is covered under CGL policies. So now, corporate policyholders and even municipalities are looking to insurance companies to bear the unbudgeted-for burden of their environmental clean-up costs. And these rulings extend not only to Superfund, but some of them also cover the Clean Water Act.

While it is true that Congress has not reauthorized Superfund legislation since 1994, insurers still need to monitor the situation. Whether or not the US Congress eventually revamps the Superfund legislation all together, Underwriters' obligations will result directly from state insurance/common law and not from federal mandates. Therefore, insurance companies will still bear the unanticipated burden of paying CGL policyholders in some states.

Perhaps in an effort to regain some control in the environmental field, many insurers have begun to sell "environmental insurance." Many of the major carriers now offer this coverage so that if a policyholder discovers contamination, the insurer can help to defray the costs of remediation. It can be quite attractive, obviously, to business owners who want to cap their own responsibility for potential clean-up costs and who want to ensure that their property retains value.

The various environmental policies include: pollution legal liability, which covers claims for bodily injury, property damage and clean-up costs; environmental remediation insurance, which only covers clean-up costs; remediation stop-loss insurance, which caps the owner's responsibility for a project's remediation costs; and post-remediation liability insurance, which covers the cost of additional clean-up work ordered by governmental authorities. All of these policies will be sold in an effort to recoup many of the losses that the industry suffered from the "sudden and accidental" court decisions of the past. In the interim, claims will continue to be made and will need to be managed prudently, expeditiously and economically on a total loss cost basis.

Gun Liability Coverage

Guns have become a growing and persistent issue in the courts and for Underwriters alike. In the 1970's and 1980's, lawyers had brought suits against gun makers making the product liability claim that handguns were defective as designed because they were harmful to society. Courts rejected these claims. They're supposed to be dangerous. These lawyers won only if guns didn't work or if they malfunctioned causing injury to the user.

More recently, lawyers have tried a new approach under negligence law. They have argued that in marketing their lethal product, manufacturers are in essence inviting or encouraging the criminal use some people would make of their guns.

In essence, the suits against the manufacturers have broken down into two categories. The first type of suit is by cities and municipalities arguing that the manufacturers should provide restitution for the police, medical, and other costs that they've incurred as a result of gun violence. New Orleans, Miami, Bridgeport, Chicago, New York, Philadelphia, Cincinnati, Los Angeles, San Francisco, Cleveland, Detroit and

Atlanta have all filed suits against manufacturers. Bridgeport sued for $100 million dollars. Chicago's suit names 16 gun stores and 22 manufacturers, and seeks $4.33 billion. Chicago claims that these defendants over-saturated the Chicago market, providing more guns than could possibly be needed lawfully.

The second type of lawsuit is filed by private individuals who allege that the manufacture and sale of guns have resulted in bodily injury from a particular shooting or series of shootings. Some plaintiffs have argued that the manufacturer should have required the use of a trigger lock, or placed warnings right on the weapons. Others have argued that the manufacturer knowingly sold weapons to people who were likely to use them illegally. Notably, courts have been very receptive to these suits, finding that traditional tort law principles encompass a "duty of care" on the part of gun manufacturers and distributors to those injured by the criminal use of their product. For example, in February of last year, a federal jury returned a verdict that the shootings of three separate individuals had been proximately caused by certain manufacturers' negligent marketing and distribution of guns.

Needless to say, if a declaratory judgment action is not initially successful, or is stayed pending the outcome of the underlying claim, Underwriters must still be cognizant of the duty to defend costs.

In the event gun manufacturers can be held liable for what other people do with their products, may alcohol distillers be next? Like the gun manufacturers, they put a product into the stream of commerce that if used improperly, can have the propensity of making the person who has consumed the liquor, a deadly weapon. Could an argument be made that they should be placing child-proof caps on their bottles? Maybe they should be placing warnings about the dangers of drunk driving on their bottles, as well. After all, what's to stop the family of a person killed in a drunk driving crash from recovering a multimillion dollar verdict from an alcohol distiller, if the family of a victim of gun violence can recover the same from a gun manufacturer?

So what does all of this mean for Underwriters? Coverage claims will come under CGL and Product Liability policies. Because large suits are not time-specific but rather span long periods of manufacturer and sale, claims will be made under occurrence policies going back a good deal in time.

Possible defenses include:

1. whether injuries were expected or intended;

2. the product hazard exclusion, which contemplates risks resulting from liability of the manufacturer for faulty or defective products to the user of the product suffering injuries therefrom -- but the exclusion probably does not exclude failure to warn claims;

3. is it a covered loss, that is, damage resulting from bodily injury, property damage, personal injury or advertising injury? Probably not, if the damages are public security costs and municipal services. It might however cover medical costs, false advertising and nuisance.

4. Lastly, there will surely be the issue of when a policy is triggered (the negligence and the injuries may span long periods), and there will be issues of apportionment, just as with the continuing environmental and the asbestos claims.

Other Areas to Consider

Before closing, there are other potential blips on the radar screen, which cannot be ignores While litigation in these areas is still in its early stages, there are compelling reasons to believe they may give rise to the next wave of insurance claims.

The first area is electro-magnetic fields, known as EMFs for short. Equipment manufacturers, telecommunications companies, and electric utilities may find themselves part of a new frontier in coverage litigation if cases involving underlying claims for exposure to an electromagnetic field continue to be filed. While there is a paucity of any scientific evidence that EMF's cause cancer or other health risks, there is no scientific evidence that they do not cause the diseases. Potential assureds may include high-voltage power lines to cellular phones to hair dryers.

Lawsuits have already been filed by landowners and electronic industry employees against equipment manufacturers, cellular phone companies, and electric utility companies. In one case, Boeing reportedly paid $600,000 in settlement to a widow of a worker who worked with pulsed EMF and later died of leukemia. In another case, a Texas court awarded $25 million (later reduced to $8.5 million) to a school district near power lines.

A second area to keep an eye on is lead paint. With 57 million housing units in the U.S. allegedly containing lead paint, and 14 million of these believed to contain paint in poor condition, the Insurance Information Institute recently predicted that insurance companies could pay more than $3 billion for lead paint claims over the next ten years. And of course, children are the ones who are being injured.

The Centers for Disease Control has estimated that 10% of all United States preschoolers suffer from lead levels in their blood that are high enough to poison their systems. In New York City, for example, the city is already facing almost 1000 claims on behalf of children who were exposed to lead in city-owned apartments. The estimated costs to resolve just these pending cases is $500 million. There are an equal number of cases pending in Baltimore City, Maryland. In response to all of this, many insurance companies are now attempting to obtain lead poisoning exclusions in their policies.

A third area is the “sick building syndrome.” From some recent cases, it seems clear building owners may face liability for tenants’ injuries allegedly caused by contaminants which are present in the living or working space of the building. For example, a suit by a small business owner who becomes very sick might lie against the landlord who allowed him to breathe biological contaminants caused by the faulty operation of his air conditioning system. Some courts have already addressed whether the pollution exclusion might preclude cover, and have answered the enquiry in the negative.

The fourth and final area is global warming. There is new evidence global warming could lead to an increase in extreme weather events, and consequently cause more property losses. But a worst case scenario from global warming could cause a major change in what is called the thermohaline circulation – the flow pattern in the Atlantic Ocean in which water travels from the Antarctic to the Arctic. This could lead to a colder climate and significant changes in the storm tracks over the United States and Europe. It is an area deserving of continued attention.

We trust this information will be of assistance as Underwriters, brokers and claim professionals in the Market continue to evaluate the next threats to their covers, and implement creative solutions to manage them prudently. As mentioned at the outset, accurately predicting where the next wave of insurance claims is going to come from is not an easy task. However, we can make some forecasts based upon current developments and historical trends. At the end of the day, it will be the foresighted ones who will be factually enabled to provide innovative solutions, strategic alliances, and opportunities to their customers and reinsurers to write business profitably under new and improved business models.

Bernd G. Heinze, Esquire
Beacon Management Group, Inc.
989 Old Eagle School Road
Suite 805
Wayne, PA 19087
+ 610.225.2363 (office)
+ 610.225.2364 (fax)
bernie.heinze@beaconriskservices.com