CPCU SOCIETY INSURING YOUR SUCCESS 1944-2004 Celebrating the Past, Shaping the Future

Cutting Edge

IT

Volume 11 Number 3 December 2004

From the Editor

by Robert L. Siems, J.D., CPCU

■ **Robert L. Siems, J.D., CPCU,** is an insurance defense trial attorney in private practice with the Law Offices of Robert L. Siems, P.A. His focus is on coverage and claim handling issues, trial advocacy and ADR, and he consults on litigation management and risk management issues. Siems has been the National Extra-contractual Group Counsel for St. Paul Fire and Marine Insurance Company, and he previously held the same responsibility at USF&G Insurance Company. A past president of the Maryland Association of Defense Trial Counsel, he has a CPCU and an Executive M.B.A. degree. Siems regularly teaches and writes on claim handling issues and on coverage law and ADR in Maryland and nationally.

This edition of your *Cutting Edge* will reach you after the Annual Meeting and Seminars in Los Angeles has ended. Your chairman, Patricia L. Saporito, CPCU, and my co-editor, Lamont D. Boyd, CPCU, tell me that this was another highly successful and informative meeting.

Your IT Section Committee met for most of the day on Saturday, October 23. That meeting included work on your web site, your newsletter, and other areas for an even better section next year. The section has brought home a second consecutive Circle of Excellence Gold award for its contributions to the Society. This is the highest recognition from the Society for a section's work. Our sights are set on having all of our section members and committee members work together for a third consecutive gold award for 2004–2005.

This edition is focused on identity theft, agency-carrier technology issues, and structuring of information technology.

In the second part of his article, "Identity Theft: Modern Problems, Modern Solutions," Greg Nelson, CPCU, AIM, analyzes how the risk of identity theft meets the factors of an insurable peril. Insurance policies that cover the risk are discussed. Finally, prevention and protection tips are analyzed. Identity theft is a hot topic due to its rapid increase in appearance. The Federal Trade Commission found that between 2001 and 2002, complaints of identity theft rose 87 percent, and the Commission reportedly had more than 161,000 complaints of identity theft in 2003. The United States Secret Service has estimated that identity theft costs consumers nationwide $745 million each year. According to the Identity Theft Resource Center, it takes the average victim more than 600 hours to clear his or her credit record. Be sure to read Nelson's article.

The Agents Council for Technology (ACT, www.independentagent.com/act) has kindly permitted us to reprint its report, *Guidelines for Effective Agent-Carrier Technology Agreements*. The report is intended to help agents, brokers, and insurers identify issues to address in technology agreements. Used to supplement the agency agreement, good technology agreements provide identification and type of access for authorized parties, control use of electronic data and other carrier information, manage access to client data and policy data, and include warranties and indemnification.

How IT platforms are built depends on the organization of the business by which the IT structure will be used. In another great article, committee member Lynn M. Davenport, CPCU, provides her thoughts on aligning IT infrastructure to an individual business's organizational structure.

Our section is uniquely situated to grow over the next year. We have gained a new committee member, Bruce D. Hicks, CPCU. Bruce is with *Rough Notes*. He has kindly agreed to share his experience as a co-editor of the *Cutting Edge*. The newsletter's availability online is being expanded. Bruce and I hope to provide an informative newsletter to you four times next year.

The timing is great for anyone with a professional interest directly or indirectly related to information technology. The Insurance Institute of America's AIT program is great and always getting better. The Society's 2005 Annual Meeting and Seminars theme is "Get Your Career in Gear." We aspire to work together as a section to accomplish this. We are working on developing sessions on fraud for next year's national meetings. If you are interested, please contact Michael J. Highum, CPCU, at mhighum@mcgowaninc.com.

Finally, thanks are due to Douglas J. Holtz, CPCU, CIC; Glen R. Schmidt, CPCU, CLU; and Lawrence W. Lagedrost, CPCU. They are leaving our committee. Their contributions have been invaluable. Doug and Glen are joining Larry E. Fagersten, CPCU, on the Board of Governors. Their service to your Society will continue in the new capacity. On a personal note, I thank Doug for all of his help over the years. Doug and Larry took me under their wings at my first meeting in Seattle, and they are a principle reason why so much of my time has been devoted to the Society over the last three years. ■

Identity Theft: Modern Problem, Modern Solutions: Part II

by Greg Nelson, CPCU, AIM

Editor's Note: Due to length constraints this article appears in two installments. The first installment appeared in the June 2004 issue of *Cutting Edge*. The research contained in this article reflects the view of the CPCU Society's Orange Empire Chapter Research Committee and Greg Nelson, CPCU, AIM. It does not necessarily reflect the view of the CPCU Society or its affiliate chapters. The research is intended to stimulate interest in the subject covered. The CPCU Society and its affiliate chapters hereby disclaim any liability that may arise from reliance upon any of the thoughts or ideas expressed in this article.

■ **Greg Nelson, CPCU, AIM,** is a past president of the CPCU Society's Orange Empire Chapter and has been on the chapter's board of directors since 1988. Nelson has served as the Research Committee chairman for the last eight years. In that period, he has written five research papers that have been recognized by the CPCU Society for Excellence in Research. Two of those papers have been published in the *CPCU Journal.*

What Can You Do About It?

Is identity theft an insurable peril? According to a well-known insurance textbook, *Principles of Insurance*, there are seven essential criteria for a peril to be insurable. They are:

1. There are a large number of homogenous exposure units.
2. The loss produced must be definite.
3. The loss must be accidental and fortuitous.
4. The potential loss must be large enough to cause hardship.
5. The chance of loss must be calculable.
6. The peril must be unlikely to happen to many of the group at the same time.
7. The cost of insurance must be economically feasible.

Large Number of Homogenous Exposure Units

Obviously, this is true when it refers to potential victims of identity theft. Everyone in the United States has the potential of experiencing the theft of his or her name. Adults with credit records would be most likely targets for ID theft. According to the 2000 United States Census, there are 205 million people over age 18 living in the United States. Most of them would have some type of credit record, and, therefore, could be victims of identity theft.

Loss Produced Must Be Definite

If a thief creates false accounts and fraudulent credit cards that affect a victim's credit record, the event would be definite. The amount of loss might be unclear, but there is definite financial value to the time and effort it takes to correct an individual's credit. The insurance carrier can fix the amount by establishing a maximum limit on the amount that the company is willing to pay in the event of a loss.

Loss Must Be Accidental and Fortuitous

No victim has any control over identity theft. Victims of this crime appear to be somewhat random. In some cases, thieves do target specific individuals, like celebrities, and in other situations they seem to act on opportunities that they encounter. In any event, from the victim's viewpoint, the losses are completely random; therefore, they appear to meet the criteria of being accidental and fortuitous.

Potential Loss Must Be Large Enough to Cause Hardship

Although the direct financial loss to victims is usually minimal, the time and money it takes to repair a damaged credit record can be substantial. Since the amount of time and effort that is necessary to clear your credit is unknown, the real cost in not predictable. Hence, the loss caused by identity theft is an open-ended amount, and the effort can take years. In view of this, most individuals would gladly trade the set cost of insurance or loss control measures over the unknown cost of the identity theft loss.

Chance of Loss Must Be Calculable

The last couple of years, ID theft has ranged from 500,000 cases to 750,000 cases per year out of the U.S. adult population of about 205 million. It appears to be growing somewhat, but at present 0.1 to 0.2 percent of the population suffers an identity loss each year. This is very similar to the frequency rate for residential fire losses. In 1999, there were about 400,000 residential fires in the United States. According to the U.S. census, there were about 107 million residences in the United States. This works out to a frequency rate for residential fires of about 0.3 percent, or just slightly above the identity theft rate. So the incidence of identity theft is similar to that of residential fire losses. Hence, the chance of loss seems to be predictable, and with a set coverage amount, companies should be able to predict the amount of expected losses from this peril.

Peril Must Be Unlikely to Happen to Many Members of the Group at the Same Time

Identity theft requires personal data, time to apply for fraudulent accounts, and time to misuse the accounts. Each case of ID theft occurs separately. There is simply no way for a criminal to create multiple ID thefts at the same time. Hence, there is no way for many members of the general population to experience the loss at the same time. In effect, there does not appear to be any way for a catastrophic event to occur to a block of consumers that would involve identity theft.

Cost of Insurance Must Be Economically Feasible

Given the unknown amount of the cost of each loss, companies can make the product affordable by limiting the amount and types of coverage they will offer under the insurance policy. They can establish a maximum coverage amount and set the premium to make sure the coverage is affordable and attractive to consumers. Companies can also adjust the benefits of the insurance policy as required to keep the losses in line with the premium charge.

In conclusion, it appears that identity theft can be insured as it meets the seven major elements of an insurable peril. In some ways it is very similar to other insurance products, even having a loss frequency very close to that of residential fire. Several companies have validated this premise by creating coverage to provide protection for identity theft.

Identity Theft Insurance Policies

Several companies have developed policies or endorsements for existing personal policies to deal with the ID theft problem. Most existing policies like homeowners, tenants, condominium, and commercial policies do not provide any real coverage for identity theft. Many of the losses, such as credit card misuse or bank account fraud, are not really losses that can be covered by standard policies. There are also costs, such as mailing expenses, attorney fees, and application costs involved in clearing up credit records that simply do not fall under standard policy coverages. Hence, several companies have stepped into the market with coverages designed to address these issues. Chubb, AIG, Travelers, and Farmers, to name a few, have all produced an "identity theft" package of coverage. Although there are some variations in limits and coverages, all of the policies provide the same basic benefits. These benefits help pay for legal fees, time off work, and related expenses that are required for the victim to repair his or her credit record. Most of the policies set a maximum limit on the amount of money the company will reimburse victims for their efforts at clearing their credit record. This amount runs in the $15,000 to $30,000 range. Some of the carriers will allow a consumer to buy higher limits for an additional premium charge. The benefits that are provided by all of the policies include:

- replacement of lost wages for taking time off work
- notary and certified mail costs
- fees for reapplying for loans that were turned down due to the poor credit
- phone charges for calls made relative to the credit repair efforts
- attorney fees

These policies can help the consumer with some of the financial effects of identity theft. In particular, it will help pay for extra costs such as mail, attorney fees, and phone charges that victims will incur in their effort to repair their credit. Payments from these policies can also help to replace lost income victims incur as a result of missing work to respond to the problems created by the theft of their identity. These policies, therefore, can be a helpful aid in dealing with identity theft.

Prevention—The Best Solution

In spite of the fact that you can buy insurance that can help to mitigate the financial burden created by identity theft, the best way to deal with this crime is to take steps to prevent it. Keeping critical personal information out of the hands of identity thieves is the primary way to avoid identity theft. The old saying of "an ounce of prevention is worth a pound of cure" truly applies in this situation. Like many maladies of life, the best cure is never to get the "disease." There are several processes that individuals can follow in order to make it less probable that their identity will be stolen.

Protect Financial Information

The first and foremost way to prevent the theft of your identity is to protect your personal information from disclosure to others. Thieves rely on getting much of the personal information from paper documents. An individual can protect these potential sources of information through several methods. Some of the easier methods are:

1. Destroy personal documents when you are through with them. Shred them, burn them, or tear them into tiny pieces—but make sure that the information on the documents is unreadable when you dispose of the document. This would include credit card and medical statements, tax records, and utility bills. As mentioned before, many companies use your social security number and date of birth on documents as account identification numbers. Thieves use this information to steal identities and create new accounts. By simply making the information on the accounts unreadable, these sources of information will be useless to a criminal.
2. Don't give out personal information to people you don't know. When contacted by telemarketers, make it a habit to verify who they are before you share any information with them. If necessary, ask for a phone number and address and indicate that you will call them back after you "check out" their organization. It may even be a good idea to only give information to companies that you have made the decision to contact—not companies that have contacted you. This allows you to check to see if the company is a legitimate concern before you decide to do business with it. A related matter extends to the Internet. Deal only with well-known companies or companies that you have verified are real entities. Some thieves may create web sites and appear to be functioning organizations on the Internet. However, they may be using the Internet to secure personal information from unsuspecting consumers. Consumers must be very careful about sharing personal information by phone, Internet, mail, or any other method of communication.

Continued on page 4

Identity Theft: Modern Problem, Modern Solutions: Part II

Continued from page 3

3. Protect your mail at all costs. Both incoming and outgoing mail can be subject to theft and give thieves the information they need to steal your identity. Receive your mail in a locked mailbox and put your outgoing mail in a locked mailbox or a U.S. Postal Service mailbox. Although thieves can break into locked mailboxes, they will more likely look for easier targets to get personal information.
4. Check your credit records at least once or twice a year. This is a very cheap form of "insurance" for identity theft. The three major credit record companies—Equifax, Experian, and TransUnion—will provide a copy of your credit record for free or for a very nominal fee. Keep in mind that much identity theft takes place for long periods of time before discovery by the victim. According to the Federal Trade Commission, the average amount of time before a consumer discovers the theft of his or her identity is 14 months. The longer the fraud goes on, the more difficult it will be to clear up the credit record. Ordering credit records on a periodic basis will identify any new credit card accounts or loans that a thief may have opened in the name of the victim. This will enable the victim to stop the use of his or her name and start the recovery process.
5. Decline free credit card offers and request that you be removed from marketing lists. This will prevent your name from being sold with personal information to others who may misuse it. It will also stop the "pre-approved" credit card offers that consumers often receive. Some thieves take these offers and redirect them to their own address. They then use the new credit card under the consumer's name but listed under the thief's mailing address. Stopping these offers will prevent this from occurring.
6. Monitor monthly bills. All of us may smile at the thought of not getting a credit card bill or receiving a loan payment reminder. However, failure to receive a monthly credit card bill may be an indication of identity theft at work. A thief may have rerouted your bills to his or her own address. Thieves can then use your accounts or set up additional accounts in your name using the information they got from the original bill. Also, it is very important to review the monthly statements you receive on all credit card and bank accounts. Check for unauthorized activity on the account. Unauthorized transactions could reflect the work of an identity thief using your name. As mentioned previously, unauthorized use of ATM and debit cards is not limited to $50 like credit cards. Until reported to the bank, there is almost no limit to the amount a thief can steal using these cards—and the money comes out of your own bank account—it is not charged to the bank.
7. Keep extra personal information out of your wallet. In most states it is required that you carry your driver's license with you when you drive. However, there is no need to carry your social security card or social security number with you. Also, minimize the number of credit cards that you carry with you. Thieves cannot only use the cards for fraudulent purchases if they should steal one, but they can also use them to create additional credit card accounts under your name. Keeping as little personal information as you need in your wallet will help to prevent identity theft from occurring.
8. Hold your mail when you are on vacation. Have a friend, neighbor, or relative pick up your mail, or have the post office hold it while you are away from home for an extended period of time. Mail piling up in your mailbox lets a thief know that you are not at home. This tells thieves that they can break into your home and steal from your home, or that they can take your mail without your missing it. They can get the personal information they need from items they remove from your home or from your mail. In a few cases, identity thieves have stolen mail, copied the personal information, and then returned the mail before the consumer was aware of the theft. Keeping your mailbox clear of mail helps to mitigate the potential of this occurrence.
9. Share personal information only with those who need it. Twenty percent of identity theft is done by someone known by the victim. Do not share personal information with anyone who does not need to have that information. At the same time, keep your personal information such as bills, statements for accounts, etc., out of sight in a secure place so it does not become an easy target for a burglar or someone who visits your home to steal.

No one can take action that will absolutely guarantee that he or she will never have his or her identity stolen. However, following these tips for loss prevention will go a long way in protecting your personal information and preventing you from becoming an identity theft victim.

Other Helpful Tips for Dealing with Identity Theft

There are a couple of additional ways individuals can help to prevent or minimize the impact of identity theft. As mentioned before, identity theft insurance can be purchased to help reduce the financial impact of this crime on the consumer. Individuals can also buy credit card protection coverage from independent companies. These companies offer a service that cancels all credit cards and orders replacement cards if your wallet or purse is stolen. The service also pays for any $50 charges the consumer may be liable for as a result of someone fraudulently using his or her credit card. This may not be necessary since most credit card companies do not hold consumers responsible for charges on a stolen or lost card if the theft is reported immediately. However, it does provide a

convenient way for consumers to deal with the theft of a purse or wallet with multiple credit cards in it. Many credit card companies offer a similar benefit for an additional charge on their cards as well. The benefit of the independent protection companies is that all the stolen cards can be handled with one phone call to just one company.

In addition, there are now some companies that provide a service to monitor the credit of individuals on a regular basis. This "credit watch" service notifies the consumer immediately if any suspicious activity appears on the consumer's credit record. Experian offers a service called "Credit Manager," Cendant offers a service called "Privacy Guard," and Citibank customers can sign up for "CreditNotify℠" to watch their credit records. These are just a few of the vendors that offer this service.

These services do not prevent identity theft but they do help the consumer with some of the processes necessary to correct identity theft problems. They also help to mitigate the personal financial cost to consumers should their identity be misused.

If You Become a Victim

A consumer can follow all of the above prevention techniques, buy an identity theft insurance policy, and secure credit card protection and credit watch service and still be victimized by an identity thief. Once the thief secures critical personal information he or she can take on the consumer's identity or create new accounts in the consumer's name. For some time the consumer may not be aware of the problem. However, it is very important that the consumer address the issue as soon as he or she becomes aware of it. Following is a list of the key steps a consumer should follow if he or she becomes a victim of identity theft:

1. Contact the Federal Trade Commission to report the situation.
2. Contact the local post office if the mail was involved.
3. Notify the Social Security Administration if the social security number was used in the theft.
4. Notify the IRS if there is the potential that taxes may be affected.
5. Contact the three major credit bureaus—Experian, Equifax, and TransUnion—fraud units.
6. Advise all of your credit card companies.
7. Contact all banks, credit unions, stock brokers, and other financial entities where you have accounts.
8. Contact check verification companies to warn them of the potential of fraudulent checks.

Notifying all of these agencies and organizations will be critical in stopping identity fraud and in starting the process of fixing your credit record. It will be a long and tedious process, but prompt action by the victim will reduce the amount of time, effort, and money that will be needed to repair the damage to his or her identity and credit record.

Summary

Identity theft is a growing crime in the United States. It has been "fertilized" by the growth of the Internet. Many identity thieves have become more active because the Internet has given them anonymity that they did not have previously. The Internet also gives thieves the ability to secure personal information they need to commit identity fraud. However, even without the Internet, identity theft would be a serious problem for our society, occurring almost as frequently as fire losses do.

There are many ways to deal with ID theft. Consumers can buy credit card protection. They can sign up for "credit watch" services that will monitor their credit and identify unusual activity on their accounts. Consumers can also buy insurance for identity theft, not unlike insurance they purchase for homes or vehicles. Identity theft insurance and credit protection services can compensate consumers for some of the expenses they incur in trying to restore their name and their credit after someone has used their identity fraudulently. However, insurance and credit protection services cannot return the hours of effort and the lost time consumers must use in order to repair their blemished credit record. For this reason, the best technique for dealing with identity theft is to take steps to prevent it from ever happening. Some simple preventive steps can make it more difficult for a thief to steal one's identity. Although the chance of identity theft can't be completely eliminated, these simple steps can reduce the risk of identity theft significantly. If consumers can protect themselves from identity theft, they will save assets much more valuable than money—they will save their time and their piece of mind. ■

Endnotes

1. Mehr and Cammuch, "Principles of Insurance," Richard Irwin Publications, 1976, p. 34.
2. National Fire Data Center, "Residential Fire," National Fire Protection Association, November 9, 2001.
3. Federal Trade Commission; "Identity Theft Complaint Data," FTC Publication, January 2001, p. 4.
4. Ibid.

Contact Information

Credit Reporting Agencies

Equifax
(800) 685-111

Experian
(888) 397-3742

TransUnion
(800) 888-4213

Social Security Fraud Unit

(800) 269-0271

Internal Revenue Service

(800) 829-0433

Federal Trade Commission

(877) 438-4338

Check Verification Vendors

Check Rite
(800) 766-2748

Equifax
(800) 437-5120

National Processing Center
(800) 526-5380

SCAN
(800) 262-7771

TeleCheck
(800) 710-9898

Guidelines for Effective Agent-Carrier Technology Agreements

An Agents Council for Technology Report

by members of Agents Council for Technology—Technology Agreements Work Group

Editor's Note:
The Agents Council for Technology (ACT) (www.independentagent.com/act) is an association of agents, brokers, users' groups, carriers, vendors, and industry associations dedicated to encouraging and facilitating the most effective use of technology and workflow within the independent agency system. ACT is affiliated with the Independent Insurance Agents & Brokers of America, Inc. (IIABA).

This report was prepared by the ACT Technology Agreements Work Group and is reprinted here with permission.

Introduction

The level of electronic interaction between agencies and carriers has increased dramatically in recent years, and this pace is likely to accelerate. In this environment, ACT believes it is important that agent-carrier agreements accurately address the expectations and commitments of the parties on these technology issues.

As part of its research in developing this report, ACT reviewed the technology agreements provided by several carriers. The work group performing this analysis concluded that these agreements—where they existed—have not kept up with the new electronic relationships that are being forged today between agencies and carriers. The agreements reviewed were "all over the lot" in the scope of issues that they addressed, and many seemed to be adapted from technology software agreements that did not take into account the unique aspects of our distribution system.

This report identifies the key principles that should be included in these technology agreements. It is written from a business point of view by agents and carrier representatives who are on the front lines of implementing new technology solutions for their agencies and companies. It is not intended to be a legal analysis, but a tool for agents and carriers to use to identify the types of issues they should cover in these technology agreements. This report is *not* a substitute for agents and carriers carefully and independently reviewing their specific agreements with their legal counsel and is not a recommendation that a contract be signed or rejected.

General Issues

Some carriers have separate agreements or amendments to handle their technology issues that are incorporated by reference into their agency agreements. Other carriers include these issues directly in their agency agreement. The approach really does not matter. What's important is that these two agreements do not conflict with each other and that the principles and protections provided to the respective parties in the agency agreement are not taken away in the technology agreement, just because the agent happens to be using an electronic medium. For example, just as an agency agreement should provide that the carrier will stand behind the agent when the agent reasonably relies on incorrect policy information provided by the carrier on the paper policy or over the phone, the carrier should also stand behind the agent if the agent accesses incorrect policy data from the carrier's web site.

The work group also felt that these technology agreements should focus on the key principles and that detailed instructions should be handled using separate procedures documents that can be modified more easily as technology evolves. These procedures documents should not be used to modify the major rights and duties of the parties but are appropriate for implementing updates and revisions. Focusing on the key principles will also generate a greater understanding of the agreement's requirements by agents.

The relationships that agencies have with their carriers are central to their respective businesses. These relationships can be enhanced by the effective use of technology. It is imperative, however, that the parties exercise the same degree of care when doing business online that they use in their offline business dealings. This means, for example, that online agreements between the parties should be clearly labeled as such and should require that only authorized representatives of the parties enter into the agreements. Any online agreements should be printable so they can easily be re-reviewed by the parties. And, the "signing" party should carefully review the text of the agreement prior to agreeing to its terms, just as would be appropriate for an agreement presented to the agent on paper. Agents with questions or concerns should be able to contact the carrier and discuss these issues, as well as any modifications the agent proposes. In this way, the parties benefit from the expediency offered by the available technology while still having the ability to review and comment upon the agreement, just as they would with a written document.

Agency and Carrier Responsibility to Limit Access to Authorized Users

The technology agreement should spell out each party's responsibility to ensure that only current, authorized personnel access the carrier's web site. The agency should have the right to identify who will be an authorized user. An agency systems administrator should actively manage the logon privileges for that agency, and agency procedures should ensure that the access of former personnel is terminated immediately and similar procedures should be in place for carriers. Agency personnel should be instructed to keep their passwords confidential and not share their passwords with any other party.

Careful agency control and safeguarding of passwords that are used by its employees is a critical agency security measure to protect the agency's customer data.[1]

ACT recommends as a best practice that the agency administrator periodically check the agency's systems and carrier web sites to make sure only authorized users have access.

ACT recommends several best practices for carriers in the password management area: implement controls to authenticate the identity of the agency administrator, periodically verify with agencies that user IDs reflect current agency personnel, and check that IDs that have been submitted for termination have in fact been terminated. Carriers should also design their web sites to permit the agency to provide restricted access to specific elements of the site for particular employees rather than to provide just all or nothing access to the site for agency employees.

When a customer accesses a carrier's consumer web site directly, authentication of the user should be the carrier's responsibility since the carrier is handling the password process. As methods are developed to permit customers to logon to the agent's web site and then gain direct access to the carrier's site, the respective responsibilities of the parties for authentication will need to be determined based upon how the process works and which party controls the password process.

Agency Rights to Use Electronic Data and Other Carrier Information

The technology agreement should spell out the kinds of information and data on the carrier site that the agent is permitted to use and share with other parties for marketing, underwriting, loss control, etc. The agreement should also define the kinds of information the agency must seek permission to use or may be viewed only by the agency. In addition, any restrictions on the use of information should be clearly spelled out on the carrier web site for all agency personnel to see. Any such restrictions should not authorize less use of the information than the agent is entitled to under the agency agreement. It is important for agents to train their personnel regarding any restrictions in the use of carrier web site information.

Some carrier agreements state that the carrier "owns" all of the software and content constituting its web site and that the agent may not share any of this content with a third party, or requires specific permission to do so. This is understandable with respect to the site's software and trademarks, but it is overly restrictive with respect to the agent's right to use client and policy data from the site. Such agreements are examples where the carriers seem to have adapted technology software agreements and have not taken into account the fundamentals of the agent-carrier relationship. There is little question that the agency could use the client and policy data if it had obtained it from the paper policy or had received it over the phone from the carrier. Why should it be different if the agent accesses the data using an electronic medium—the web site? Moreover, such a restriction on the agent's use of client and policy data conflicts with the agent's ownership of expirations provision in the agency agreement. The ACT work group recommends that carrier "ownership" language not be used with regard to the client and policy data on the carrier web site because it will just generate agency concerns and confusion.

Access to Client and Policy Data by Active and Terminated Agents

Carriers are anxious to "turn off" the policy paper that agents have traditionally received and for the agents to rely on the carrier's web site for this information. In conflict with this objective, however, is the language typically found in current technology agreements, which provides for the termination of access to the carrier's site as soon as the agent's relationship with the carrier terminates. This is a great illustration of how the agreements have not kept up with the changes in how business is now being done.

Technology agreements must provide agencies with explicit protection that they will have continued access to client and policy data (covering the period when they were the agent on the risk) for no less than the period of time that state law requires them to retain such information, even if another agent takes over the business through an agent of record letter, the agency is terminated, or the status of the carrier changes (is acquired, withdraws from the line of business or state, or becomes insolvent). This information should be available in a usable format to the agent, which may include, but is not limited to, electronic access or print image. Carriers may archive the information or retain it in different formats after a period of time as long as they commit to produce the information for the agent promptly when requested. Some carriers may meet this commitment by de-linking electronic policy view from other parts of their web sites. Others may provide the agency with a CD containing the information in a usable format to the agent. Such CDs should also employ a logon/password key that protects the agency's information from unauthorized access.

It is also important for the carrier to provide the agent, using electronic policy view, access in unalterable form to the actual policy forms and endorsements that were in effect when the risk was written. These documents will be required should the agent be called upon to produce the documents for a legal or administrative proceeding.

If carriers make this commitment of continued limited access to client and policy data to their agents, they will convert their web sites from the convenience that they are today to an integral business tool that agencies can rely upon, which will generate increased agency support for carrier initiatives to "turn off" the paper.

Continued on page 8

Guidelines for Effective Agent-Carrier Technology Agreements

Continued from page 7

Warranties and Indemnification

Most technology agreements provide agents with little or no recourse should the carrier's systems or web site cause damage to the agency's systems or business. In contrast, some of these agreements require the agent to indemnify the carrier should a loss arise if the agency's use of the carrier's systems causes the carrier damage. Other carriers limit the indemnification to the agent's "intentional or grossly negligent" failure to adhere to the carrier's conditions for use of its technology. Agents need to carefully review these indemnification provisions because they vary considerably from carrier to carrier, and they should be balanced and fair, and may impact the application of the indemnification provisions in the underlying agency agreement to technology-related issues.

It is apparent from a review of current agreements that carriers have concluded that providing warranties and indemnification protection to their agents for damages caused by their technology is inappropriate, even though they provide their agencies with indemnification for their other activities in their agency agreement. Shouldn't the same reasoning apply to requiring indemnification from their agency sales force regarding technology errors? Will not such requirements discourage agents from embracing the carrier's new technology? Would not a better approach be to train the agents on these required procedures and then to audit them when appropriate? Most agencies are not in the position to indemnify their carriers, especially in an area where the risks posed by technology are still emerging and not fully understood.

If indemnification provisions are included, they should be balanced and fair, providing the same protection to each party.

The ACT work group did feel that agents should be able to rely on the client and policy data residing on the carrier's web site, just as they have been able to rely on the information contained on the paper policy or communicated by phone by a carrier employee. The group felt that the carrier should continue to indemnify for such incorrect information that the agent relies upon and subsequently causes a loss. The fact that this data is displayed on a new medium—the web site—should not make a difference.

Commitment to Prompt Correction of Data and Systems Errors

As discussed in the previous section, both agencies and carriers should take reasonable steps to protect their own systems from errors and problems caused by their business partners. It is, however, important for agencies and carriers to have a sense of urgency in correcting problems when they are found. Such problems as corrupt download files and inaccurate information on a web site might cause difficulties for their business partners. Just as for carriers, agencies have become totally reliant upon their systems to do business. The technology agreement should contain a provision where both parties commit to use reasonable efforts to resolve data errors and systems problems affecting the other party on a priority basis. Once a party discovers a data error or systems problem, he or she should communicate it to all affected parties. Where the issue involves inaccurate downloads, the carrier should work with all affected agencies to identify the historical inaccurate downloads and provide corrected downloads.

ACT recommends that the carrier provide its agents with a customer support initiative as a best practice. This initiative should clearly spell out the carrier's standards for providing support to its agency users and should include the people or departments agents may contact if they encounter problems.

Document Retention

Most technology or agency agreements provide important guidance on the types of documents that the agency is responsible for retaining. Some of the provisions, however, require the agent to keep these documents in a paper format along with the customer's "wet" signature. Given the trend of agencies to retain their information electronically, ACT believes agencies should be given the option to retain these documents electronically where permitted by state law, provided the agency retains this information in a format that is not modifiable, backs it up, and can produce it promptly when requested. In addition, all document retention requirements included in technology or agency agreements should be clear as to when the retention period begins (e.g., on a specific date or on the occurrence of a specific identifiable event) and it should be reasonable as to duration.

Third-Party Information Reports

Some technology or agency agreements spell out the agency's responsibility to obtain the consumer's permission if required before collecting this type of information (i.e., insurance scores, MVR's, C.L.U.E.™ reports), along with the need for agency personnel to use the information only for the business purpose for which it was collected.

Carriers should fulfill their own adverse action disclosure and compliance obligations directly and not shift these responsibilities to agents by contract or other means.

Conclusion

This document and the needed provisions in technology agreements will continue to evolve as new electronic interactions are implemented among agencies, carriers, and consumers. A more effective use of technology in our distribution system is critical to secure our long-term competitive position. The technology agreements that are developed should encourage the parties to embrace this new technology by being balanced and as simple as possible. They should respond to the needs of both agencies and carriers and clearly communicate the responsibilities and commitments of each of the parties. They should avoid arcane

and complex provisions that will just compound the concerns and confusion that agencies already have with implementing new technologies that they do not fully understand or that undermine the ownership of expirations or other provisions in agency agreements. The challenge for those drafting these technology agreements is to draft them in a manner that increases agency understanding of what is required of them and gives them assurances that using these new carrier electronic services is a positive move for the agency to take—rather than a move that puts the agency at greater risk. ■

Endnote

1. Training in agency security issues is very important for those employees or consultants who help the agency frame its password management policies. Please see ACT's Password Guidelines and various security related articles, improvement tools, and reports for more specific guidance on password management. These are found on the ACT web site at www.independentagent.com/act.

Congratulations to the Information Technology Section

for being recognized with the
Gold Level Circle of Excellence Recognition Award!

■ *David L. Mowrer, CPCU, CLU, ChFC, (third from right) accepts the Circle of Excellence Gold Award at the Annual Meeting and Seminars in Los Angeles on behalf of the Information Technology Section.*

CIRCLE OF EXCELLENCE
RECOGNITION PROGRAM

Aligning the IT Infrastructure with Organizational Hierarchy

by Lynn M. Davenport, CPCU, AIC, AIM, AIS, AIT

Lynn M. Davenport, CPCU, AIC, AIM, AIS, AIT, is a claim team manager with State Farm Insurance Companies in Greeley, Colorado, whose team of specialists handle water claims for policyholders in three states. Davenport, who has been with State Farm in the claims and technology arena for 16 years, previously was a project manager responsible for implementing new claims technology and processes; and also managed a team of innovators who supported claims technology and processes. She earned an M.B.A. in knowledge and learning management through Walden University in 2004; and a B.A. in psychology from St. Mary's College, Notre Dame, Indiana. A member of the CPCU Class of 1999, Davenport is an active member of the Colorado Chapter as well as the IT Section Committee. She served on the CPCU Society's Distance Mentoring Task Force, and was recently appointed vice president of Walden University's Sigma Iota Epsilon (SIE) business honors chapter. In her spare time, she enjoys mentoring, skiing, shopping, traveling, and spending time with her husband, Dave, and their two children.

Many companies have migrated to a flattened organizational hierarchy with self-empowered teams. In this hierarchy, leaders develop strategic business goals while employees set related departmental goals and determine how to accomplish those goals. Virtual teams may also play a role in the structure. Teams may include ongoing work units or short-term project teams or committees. Knowledge sharing, collaboration on decision-making, and access to relevant reports and data are necessary for the success of self-directed teams in this structure. Technology should be available to enhance the productivity and effectiveness of teams, and to help top leaders maintain awareness of what's going on in the company without micro-managing the teams.

To support the flattened team hierarchy, an IT infrastructure should include several key elements, including:

Technical and Application Infrastructure

- Knowledge-base systems that incorporate FAQs, common problems and solutions, search capabilities, references, and policy guidelines. This helps knowledge workers share experiences and learn from others (Ruddy, n.d., p. 9).
- Integrated, centralized databases of customer information and logs of customer contact preferences/problem situations so customers won't have to repeat their situation twice to different team members.
- Shared network drives and electronic document storage archives for readily accessible project or research documents. Automated backup and recovery systems from the shared drive will help avoid lost data when an individual team member's hard drive crashes (Haag, 2004, p. 336). Document management is necessary for legal reasons and employee access to historical information (Haag, 2004, p. 343).
- Collaborative software such as NetMeeting, project management software, and online calendaring and scheduling software. Also workflow applications that provide team work queues, digital imaging features, and electronic activity logs of team activity on the file (Haag, 2004, p. 344).
- Enterprise resource planning software (Haag, 2004, p. 353), a secured intranet and self-service administrative software such as the ability to review and modify employee benefits and department budgets, request vacation, view company event calendars, access internal policies, read company news, submit expense accounts, participate in online learning, etc. (Ruddy, n.d., p. 9).
- Decision support systems to help teams analyze all relevant perspectives and to encourage innovative solutions (Haag, 2004, chapters 4 and 7).
- Portal applications to integrate cumbersome systems administrative functions such as single sign-on for multiple applications and secured access based on a team member's role (Ruddy, n.d., p. 9).
- Real-time access to production data and statistical reports so teams and management can constantly adjust the staff and production to meet goals.
- Internet access to the World Wide Web for a wealth of external information about competitors, vendors, and suppliers, etc.
- Telecommunications equipment and integration with a digital network for call centers and virtual teams. Sophisticated phone networks can enhance the team's ability to function in teleconferences and videoconferences.

- Possible extranet connection for vendor/supplier transactions with empowered teams. Use of EDI in business transactions and record-keeping.

Support Infrastructure:

- With the technical requirements listed above, 24x7 support is also needed. Easily accessible online technical support, telephone support, and on-site support must be available to help employees working with technology on empowered teams.
- Technical training must be offered in a variety of ways for teams. This may include online training, classroom training, or self-study training.
- Information security and privacy must be a priority. Clearly defined policies should be available and enforced for all employees. A secure network, virus protection software, and various spam filters will help create a secured environment that protects employee and customer information.
- Any technology deployed must be adaptable and customizable so employees can maximize its use for their specific needs and the customer's needs.
- Disaster plans must be in place so team members know exactly what to do and where to go in the event of an emergency situation. This may mean working from home on their laptop, or temporarily traveling to a hot site or cold site (Haag, 2004, p. 337). ■

References

Haag, S., Cumming, M. & McCubbrey, D. (2004), *Management Information Systems for the Information Age,* (4th Ed.) McGraw-Hill: New York, NY.

Ruddy, T. (n.d.), "Leveraging Teams and Technology to Share Knowledge," Retrieved September 30, 2003, from Google search site at http://www.google.com/search?hl=en&ie=ISO-8859-1&q=empowered+teams+and+technology.

2004 Annual Meeting Seminars Developed by the Information Technology Section

■ *"Agency-Company Automation and Technology Compatibility" panelists discussed how independent agents and the companies they represent can ensure automation compatibility.*

■ *"Business Continuity Planning—An Information Technology Perspective" panelists discussed the crucial issues of crisis management planning, emergency response and business resumption, and rebuilding an organization.*

Watch your next issue of *Cutting Edge* for details on the Information Technology Section seminars held at the CPCU Society's Annual Meeting and Seminars in Los Angeles.

SYSOut

by Patricia L. Saporito, CPCU

■ **Patricia L. Saporito, CPCU,** chairman of the IT Section, is a senior property-casualty insurance consultant for Teradata where her responsibilities include business development, business strategy consulting, and strategic alliances in the property and casualty area.

The Annual Meeting and Seminars was another stellar event for the IT Section! We participated in the "Mock Trial: Who Pays When the Sky Falls." This was a highly entertaining and educational event. In addition we sponsored two sessions: "Agency-Company Automation and Technology Compatibility" and "Business Continuity Planning—An IT Perspective." Thanks to outgoing IT Section Committee member Douglas J. Holtz, CPCU, CIC, and to Michael J. Highum, CPCU. Christopher H. Ketcham, CPCU, spearheaded our review and analysis of the information technology survey the IT Section chaired; look for a summary of the findings in upcoming newsletters. Congratulations to the entire IT Section—we brought home the Gold again for the Circle of Excellence—the second year in a row. David L. Mowrer, CPCU, CLU, ChFC, did another outstanding job in collecting and submitting our collective efforts for evaluation. Keep sending Dave your e-mails on all of our accomplishments! Also stay tuned for a new feature both in the newsletter and on the IT section web site, tentatively titled "IT Tips and Tricks," which will focus on more end-user, every-day practical IT recommendations. ■

What's in this Issue?

Cutting Edge
is published four times a year by and for the members of the Information Technology Section of the CPCU Society.

***Cutting Edge* Co-Editor**
Lamont D. Boyd, CPCU
Fair Isaac Corporation
Phone (602) 485-9858
e-Mail: lamontboyd@fairisaac.com

***Cutting Edge* Co-Editor**
Robert L. Siems, J.D., CPCU
Law Offices of Robert L. Siems PA
Phone (410) 366-5606
e-Mail: bobsiems@lawrls.com

Information Technology Section Chairman
Patricia L. Saporito, CPCU
Teradata
Phone (201) 941-2330
e-Mail: patricia.saporito@teradata-ncr.com

Sections Manager
John Kelly, CPCU, AIT
CPCU Society

Managing Editor
Michele A. Ianetti, AIT
CPCU Society

Production Editor/Design
Joan Satchell
CPCU Society

CPCU Society
720 Providence Road
Malvern, PA 19355-0709
(800) 932-CPCU
www.cpcusociety.org

CPCU SOCIETY INSURING YOUR SUCCESS Celebrating the Past, Shaping the Future

Cutting Edge

IT

Volume 11 Number 3 December 2004

CPCU Society
720 Providence Road
Malvern, PA 19355-0709
www.cpcusociety.org

PRSRT STD
U.S. POSTAGE
PAID
BARTON & COONEY