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

Cutting Edge

IT

Volume 11 Number 2 June 2004

From the Editors

by Lamont D. Boyd, CPCU, and Robert L. Siems, J.D., CPCU

■ **Lamont D. Boyd, CPCU,** is insurance market manager, Global Scoring Solutions, Fair Isaac Corporation, and is recognized as one of the industry's leading experts in predictive scoring technology. He is past chairman, and current committee member, of the CPCU Society's Information Technology Section.

■ **Robert L. Siems, J.D., CPCU,** is in private practice with the Law Offices of Robert L. Siems, P.A. He is founder and president of GF Practices, Inc., a consulting company specializing in litigation and risk management to the property and casualty industry as well as other businesses experiencing litigation exposures.

This is our second newsletter in 2004, and we have covered an array of issues. We look at identity theft, evaluate security and access in the workplace, and examine whether today's technology more often produces commodity software and hardware rather than innovation.

The article on identity theft is being delivered to you in two parts. Titled "Identity Theft: Modern Problem, Modern Solutions," this article was submitted by the CPCU Society's Orange Empire Chapter in 2002. It remains timely. The article was researched and written by Greg Nelson, CPCU, AIM, past president of that chapter and a member of its board since 1988. We are grateful for his careful research and analysis. He starts from the perspective of how identity theft takes place and the kinds of problems that it creates. These include financial costs, tremendous loss of time for the victim, and damage to reputation. The next issue will bring you his treatment of what to do with identity theft.

Lynn M. Davenport, CPCU, AIC, AIM, AIS, AIT, has written a very good article on security and access control in the workplace. This is her second piece this year, and one that you want to read and remember.

We have also included an article that was generated from a February 27, 2004, Wharton Technology Conference. Wharton is the business school at the University of Pennsylvania, and it produces a great electronic newsletter. Wharton has generously allowed us to use an article in the past, and it has again agreed to share this most recent piece called "Information Technology: Value Creator or Commodity?" IT pundits who attended the conference discuss whether IT dollars are better spent on commodity software and hardware or on IT innovation.

This newsletter follows up on agency use of IT. Summary of the recent announcement by the IIABA on its launch of "Big I" market version 1.2 is included. We have also followed up on last issue's report on use of the System Electronic Rate and Form Filing (SERFF) developed by the National Association of Insurance Commissioners. That systems use is increasing.

A recent survey by ILOG, Inc. and ACORD on our industries' response to the newest regulatory and corporate governance business demands such as HIPAA and Sarbanes-Oxley Act is included.

A summary is also included on a recent Sapiens SERFF survey on the nearsighted view of insurers on IT decisions.

Our web site guru, Lynn M. Davenport, CPCU, AIC, AIM, AIS, AIT, has kindly offered a piece on a feature of our IT section web site. Webcasts on demand are available, and you will want to read what Lynn has to say about this feature.

An IT committee spotlight is included. We are very fortunate to now have Glen R. Schmidt, CPCU, CLU, FLMI, on our committee.

Finally, your chairman has provided a summary on the seminar sponsored by your section during our most recent Annual Meeting and Seminars. That seminar covered "Leveraging Third-Party Data." Pat was also instrumental in the production of the seminar. Her work is greatly appreciated!

Your next issue of *Cutting Edge* is in the works. We are doing our best to meet the challenge of providing you with a product consistent with the high expectations that this professional Society, celebrating its 60th anniversary year, requires.

Please feel free to e-mail Lamont or Bob with any ideas for upcoming issues. Lamont's e-mail address is lamontboyd@fairissac.com and Bob's email address is bobsiems@lawrls.com. ■

Information Technology: Value Creator or Commodity?

Editor's note: This article was originally published on March 25, 2004, and is reprinted with the permission of Knowledge@Wharton. Visit its web site at www.knowledge@wharton.upenn.edu.

Only a few years ago, companies put a high priority on coming up with innovations in information technology. A new solution, software program, or piece of hardware could almost guarantee these companies a competitive advantage, at least in the foreseeable future.

Yet as companies started to realize that information technology was becoming a necessary part of their businesses, these windows of opportunity for short-term advantage began to disappear. IT innovation became easily duplicated, and IT, while clearly necessary, began to look like just another commodity.

Indeed, members of a panel on "Creating Value through IT: Is There Value In It?" held during the February 27, 2004, Wharton Technology Conference, noted, ironically, that as companies' information technology spending has increased, investment in IT, at least on a percentage basis, has gone down.

"By some measures, IT is 50 percent of corporate capital spending," said Steve Berez, vice president, IT Practice, at Bain & Co. "Yet the majority of the dollars a company spends on information technology"—about 85 percent, he estimates—"is for commodity software and hardware . . . while maybe 15 percent will go into finding something innovative." The question, Berez added, is whether that 15 percent is going to produce a strategic advantage. "The 85 percent better be working or you will not keep up with your competitors. But the other 15 percent, who knows?"

Business writer and consultant Nicholas Carr was skeptical that innovations in information technology are worth the effort these days. "When does information technology innovation make sense?" he asked. "I think for the vast majority of companies, it won't. There is a little fairy dust at the top (when it comes to innovation), but it's mostly an illusion. . . . That 85 percent Steve talks about is moving to 86-88-91 percent; it is the IT you need to keep your company going that everyone else has," he said. For the most part, companies that think they "can innovate their way to success" are wasting their money.

> *By some measures, IT is 50 percent of corporate capital spending.*

Perhaps a decade or two ago, a company could get a competitive advantage by innovating, Carr added. For example, the first banks to use online or computerized banking may have won over a number of new customers. "Now banks virtually give that away. It's just a commodity everyone has." Another example, he said, is Reuters, the news and financial information service, that was the first to come out with a big computerized network. Now every local newspaper is on the Internet.

According to Carr, what has changed is that companies rely on vendors—either software or hardware companies or consultants—to keep them current with IT rather than the companies themselves innovating for advantage. "Companies realize that retaining parity is necessary, but they are looking at IT as a commodity input. The trend is that they are getting away from thinking they can innovate their way to competitive advantage."

Still, even Carr admitted there are counter examples. He cited Wal-Mart, which has the resources and corporate drive to achieve an even greater advantage through innovation than it already has. Matthew Carey, vice president of Wal-Mart's technology and information systems division and a conference panelist, noted that Wal-Mart does 90 percent of its information technology in-house—a huge percentage given that many companies, large and small, are moving more toward outsourcing or using IT consultants.

Wal-Mart also has the advantage of being so big that its customers have to comply with its standards rather than try to impose other ones on Wal-Mart. "Wal-Mart is one of the rare exceptions," said Carr. A company of its size can actually get vendors to do some of the innovative work for them. If a company wants to sell to Wal-Mart, it might well take on that extra IT work in order to get Wal-Mart's business.

Carey, for his part, did not deny the contention, noting that Wal-Mart wants to work with its suppliers to have everyone on board with the same IT systems. "We provide tools for suppliers, sometimes at a fairly significant cost to us," said Carey. "We feel then they can leverage this and use the data to both our advantages. It may be hard to measure, but when we do a business review with a buyer and this system (is in place), then you don't have to debate the data. It saves time. That's where good IT can help."

Wal-Mart's big current information technology push is Radio Frequency Identification (RFID), a wireless tracking system that includes small homing devices

on each product that allow a computer to track where it is at any time. Most of the work, according to Carey, is being done in-house, although it is still in the experimental stage. Eventually, the dream is that RFID markers will be placed on nearly every consumer item, from peanut butter jars to boxer shorts to automobiles. They will be able to track inventory from container ship to rural store shelf and thereby help Wal-Mart understand consumer buying preferences—and maybe even how the customer uses the item after it leaves the store.

Privacy issues aside for now, RFID is in its infancy, even at Wal-Mart. The company can track pallets, or cases, of goods, not individual items, through RFID. "Our initial tests were to do everything, but we are now focused on that transit functionality (tracking items from the supplier to the warehouse) first," said Carey. "That will have the highest return on investment for us. . . . As far as at the store and item level, if I showed you what a shelf-reader (the RFID device put on shelves that will be able to read the labels on individual items) looks like, you would say, 'You're going to put that in 4,000 stores?'" he said with a laugh. "There is no way we are ready with that yet."

But Wal-Mart is definitely moving toward that end. According to Carey, his technology group sits in on every major meeting, from marketing to sales to company strategy, unlike at other companies. No one in the upper echelons of the company should be misinformed about the status of anything from RFID to a malfunctioning accounts payable software program in Colorado. "In a lot of cases, we try to help the weakest store manager, the weakest district manager," said Carey. "We target the most inefficient part of the process in IT to see how to solve it. If the process works there, it will probably work elsewhere in the system."

In the end, said the consultants on the panel, it is no longer about information technology itself in the modern company, but about how companies function overall. If Wal-Mart, for example, is getting things done in IT, it is because the managers know how to run a company.

"Software is a tool. It is configurable," said Chakib Bouhdary, vice president, value engineering, at SAP America. "It all comes down to how it is being used and how you measure its value. We have seen the same software being used by two companies in the same industry. Some use it to their advantage. Some make a mess of it."

According to Berez, Bain first looks at a company to find out where it has gone wrong using what is, for the most part, standardized IT. "We start with what differentiates you as a business," he said. "We do customize software for a client. But in the end, it's how good a company is in all areas that will aid managers in using IT."

■ *We target the most inefficient part of the process in IT to see how to solve it. If the process works there, it will probably work elsewhere in the system.*

Carr agreed, noting that as information technology gets commoditized, it is ever more incumbent on companies to learn to use it well. There is no longer room to make mistakes. That may sound like a defensive position, he added, but it is no different than how competitive businesses have functioned with raw materials for ages. "If I deliver a ton of the same type of flour to one bakery as another, the first may make something wonderful out of it and the other may manage it poorly and get horrible results," said Carr. "It is the same with IT now. Management matters. Company culture matters. One company may manage IT better than another. That doesn't tell you anything about the strategic value of the IT itself.

"That's why I suggest that looking at the IT iceberg, with the small portion at the top left for innovation, may lead to foolish spending," he added. "You can say, 'Hey, I can get ahead if I get that tip of the iceberg.' I would contend that you should look at the 90 percent underneath, or you will fall way behind."

Even Wal-Mart, with all its potential in IT innovation, understands this point. "What we have found is that maybe 70 percent of the budget is just keeping the lights on, (taking care of what) we already have that we still need," said Carey. "A lot of what you do is make sure that the company maintains its business. You have to keep the lights on every night." ■

Identity Theft: Modern Problem, Modern Solutions: Part I

by Greg Nelson, CPCU, AIM

Editor's note: Due to length constraints this article will appear in two installments. The first installment appears here. The next issue of *Cutting Edge* will include the remainder of the article. 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 six years. In that period, he has written four 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.* Nelson is presently the senior vice president for Safeco Financial Institutions Solutions, a specialty division of Safeco Insurance Company, which provides insurance products and services to financial institutions.

Introduction

You hear about it every day. You read about it in the newspapers, hear it on the radio, and see it on television. No one is immune to it. It happens to people in every walk of life, from small rural towns and farms to the largest cities in the country. It affects all types of people, from those who toil at the lowest level of clerical positions to the most well-paid athletes and celebrities. Politicians and trash collectors, preachers and teachers, executives and students have all been its victims. Although it happens with regularity in the United States, the problem occurs all around the world. What is it? What pervades every part of our society and can affect anyone? What is one of most devastating "diseases" of our economic society? That "disease" is identity theft and it is growing at an incredible rate. It is part of the price we must pay for the technological benefits we have in our civilization. The same benefits that enhance our lives have also helped to make identity theft one of the fastest growing crimes in society today.

If we are to utilize the technology we have at our fingertips and enjoy the benefits it offers to us, we must learn to deal with the challenges of identity theft. This article will investigate the reasons for the rapid growth of identity theft over the last few years. It will provide cases of identity theft and the costs to the consumers who had their identities stolen. The article will analyze what the real costs of identity theft are. It will detail the obligations of victims from actions by identity thieves. The article will then analyze the steps the insurance industry has taken to provide insurance for this "new" peril. Is identity theft an insurable peril? If so, what are the elements that make it an insurable? What policies are available to address this peril and what benefits do they provide? Is insurance the only way to deal with the problem, or are there better ways to protect yourself? This article will provide a recommended list of actions the consumer can take to deal with identity theft, including contact names and telephone numbers for consumers to use if they become victims of identity theft.

The Internet—Making Identity Theft Easier

We live in a great society. Modern conveniences have made our day-to-day lives easier. We get paid well and have excellent medical care and living conditions. Technology has taken many of the challenges of day-to-day life away from us, and enabled us to do things in hours that would have taken days to do in just the recent past. We get instantaneous information on world events and up-to-the-second data on the stock market. Through cell phones we can communicate with others virtually anywhere in the world. Technology has influenced every facet of our lives.

Perhaps one of the greatest events of our time has been the development and growth of the Internet. From its beginnings in the early 1990s as a communication network between a few universities in the United States, it has grown to become one of the most useful tools in both the United States and the world. From a few users in the early years of its infancy, it has grown to the point where 66 percent of the adults in the United States—137 million people—use the Internet on a regular basis, either from their homes or at the office.[1] The Internet is most often used as a resource to gather information, but it has also become a huge marketplace where consumers can buy or sell items online. It has become a convenient place to pay bills, communicate with others, and order delivery of groceries and other household goods. It is even possible to purchase major items such as houses and cars on the Internet, to secure financing for those purchases, and to buy insurance for them without ever leaving the comfort of your home.

This ultimate convenience, however, does not come without some cost. In order for us to partake in the "fruits" of the Internet, we are forced to share information on the Internet that we have previously only provided in person or by filling out applications and other paperwork. Sharing this information online makes it more vulnerable to theft and has helped to increase the occurrence of one of the fastest growing crimes in the country—identity theft. Not only has the Internet enabled thieves to steal existing identities, but it also facilitates the creation of false identities that are then used to defraud banks, credit card companies, and other types of businesses. Transactions on the Internet do not

require face-to-face interaction. This limits the ability to verify information and validate the real identity of the buyer. This lack of face-to-face interaction makes it much easier to commit fraud and theft, and is one of the prime reasons why the incidence of identity fraud and theft has increased so dramatically in the past few years.[2]

Identity Theft—Not a New Problem

Identity theft has been around since the beginning of time. In the past, individuals impersonated persons of substance or reputation in order to secure favorable treatment or to steal something of value. But "stealing" or taking someone's name can result in more than just a theft of financial value. Shakespeare put it succinctly in the play *Othello* when he said, "But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed."[3] The same affects occur with identity theft today. The person who suffers the theft of his or her name suffers both financial and non-financial losses. Identity theft can be defined as "all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."[4] Some examples of recent identity theft include the following:

- In 1997, a retired Air Force colonel, John Stephens, was contacted by a collection agency regarding being delinquent on payments for a $27,000 Jeep Cherokee bought in Dallas, Texas. Stephens, who lived in Maryland, did not have a Jeep and had not been to Texas for more than 30 years. But his name and social security numbers were on the contract for the Jeep. Over the next few months he found out that four additional vehicles and a total of 28 other items worth $113,000 had been purchased in his name. This destroyed his previously excellent credit record, and even though he was not responsible for these fraudulent purchases, it took him three years and $6,000 in legal fees to clear his credit record. In the meantime, he was denied a loan to build a vacation home, and he had to pay cash for a new heating and cooling system because of his "questionable" credit.[5]
- Beverly Reed, whose purse was stolen, experienced similar badgering by debt collectors and denials by banks when someone stole her identity. At one point the ID thief attempted to mortgage Reed's house in order to buy a car.[6]
- In yet another case, Marc Nelson of Huntington Beach, California, found that there were outstanding loan complaints against him in Florida, even though he had never been to Florida. The identity thieves tried to access his bank accounts and to run up his credit cards. Finding fraudulent charges on his American Express card, Nelson canceled the card and secured a new one. In the following three days, the thieves had run up 50 transactions for a total of $13,000 on the canceled American Express card.[7]

These are just a few examples of the typical experience as a result of identity theft. The problem has been around for a long time. However, the emergence of the Internet as a major communication and business tool has increased the incidence of ID theft in the last couple of years. In fact, ID theft has now become the most worrisome problem for consumers in the United States. According to the Federal Trade Commission, 42 percent of its complaints from consumers are related to identity theft—far more than any other consumer complaint.[8] It is now estimated that as many as 750,000 citizens will have their identity misused this year, up from 500,000 just a couple of years ago.[9] Although consumers are not responsible for the financial obligations created by the identity fraud, it does take significant amounts of time and effort to rectify one's credit record after it has been damaged by an act of identity fraud.

On the other hand, identity theft does cost American businesses millions of dollars in losses every year. Visa and MasterCard are projecting that ID theft fraud on credit cards now exceeds $1 billion per year.[10] Even celebrities have been subject to identity theft. Well-known personalities such as Martha Stewart, Oprah Winfrey, Steven Speilberg, and Tiger Woods, to name a few, have all been victims of identity theft in the last few years.[11]

So ID theft is a problem that is growing quickly, especially because of the popularity of the Internet.

How Do They Do It?

The most frequent type of ID theft occurs when the thief gets the social security number of an individual and combines it with a driver's license number or a date of birth. Using this information, the thief can open lines of credit and bank accounts or request new credit cards in the victim's name. The thief then carefully directs the statements or cards for the new accounts to his or her address. The thief can then use the credit cards or bank accounts to purchase items or run up bills. In the meantime, the victim's good credit allows the thief to continue to open additional accounts or to continue

Continued on page 6

Identity Theft: Modern Problem, Modern Solutions: Part I

Continued from page 5

to charge on the fraudulent accounts. Only after several months do the creditors "track" the victim (the consumer) down to find out why he or she is not paying on all of the new accounts he or she has recently opened. Of course, most consumers have no knowledge of these "new" accounts, since they were created by identity theft. The consumers are shocked to find out that their previously outstanding credit has now been ruined by the activity on these new accounts set up by the identity thief.

Major Types of Identity Theft Complaints

Once thieves are able to create an account by taking a victim's identity, there are several ways in which they exploit the ID theft for their own economic gain. According to the Federal Trade Commission, the major complaints about identity theft include the following:

- Credit Card Fraud—Fifty percent of the complaints to the FTC involved creation of fraudulent credit card accounts or unauthorized use of existing accounts in order to buy goods or services.
- Phone or Utility Service Fraud—About 25 percent of consumers indicated that the ID theft they experienced involved the creation of telephone, cellular, or utility services in their (the victim's) name. The identity thief does this to avoid having to pay for the service, or to establish an address from which he or she can conduct other illegal activities.
- Bank Fraud—About 16 percent relate to issues with bank accounts, including opening fraudulent accounts, writing bad checks, or making unauthorized withdrawals from the victim's accounts.
- Fraudulent Loans—9 percent of the complaints are created by ID thieves securing a loan in the name of the victim, or using the victim's credit record to secure a loan from a bank.[12]

In most of the situations, the perpetrator creates a new account—credit card, bank, and cell phone, etc.—using the name of the victim. In order to do that, the thief must have some key personal information of the victim in order to establish the account. Most often this is the social security number, driver's license number, and the date of birth of the victim. The most valuable item of personal information that a thief can use is someone's social security number.

Social Security Number—Identification Number of Choice

The social security number has become the main tool for identification in the United States. When the Social Security Administration was created in the 1930s, the numbering system was never intended to become the primary ID number for citizens in the country. In fact, the government promised that it would never be used for that purpose.[13] In spite of that assurance, the social security number has become the key identification number used by most entities in this country. Hence, once a thief has the social security number of another person, the thief can gain access to a significant amount of personal information about that person.

There are several ways that identity thieves secure social security numbers and other personal information:

- The primary method of getting personal information is to steal the wallet or purse of the victim. Most people carry their driver's license number in their wallet or purse. Unfortunately, many people also carry their social security card in their wallet or purse as well. These two types of identification give an identity thief all the information he or she needs to begin the theft process.[14]
- The Internet is another source of personal information. Stealing a person's wallet or purse may be the easiest way to get personal information. However, some of the information is very easily secured from the Internet. A resourceful thief can "order" a social security number online for $39.95.[15]
- Another technique thieves can use is to "steal" mail from a victim's mailbox. They can then get information from bank statements, medical billings and statements, tax records, credit card statements, and other personal mail. Many of these items display social security numbers, dates of birth, and other personal information. Medical statements, college transcripts, ID cards, driver's license numbers, and some investment accounts often use the owner's social security number as the account number, which is printed on various documents. Thieves can get one of these documents and use the information to "create" fraudulent accounts. In some cases, they can send out a "change of address" form on the accounts, instructing the companies to mail future billings, statements, or information to a new address. They then start using the accounts over the phone or on the Internet. Since the victim never receives the statement on bills, several months can go by before he or she becomes aware of the problem. Usually, a call from a collection agency is the first indication of a potential problem. By that time the thief may have created thousands of dollars of fraudulent bills and virtually destroyed the victim's credit.
- "Dumpster diving" is another method of obtaining personal information. Instead of stealing mail, some ID thieves will go through the trash, looking for discarded bills, statements, and other personal information. Once the identity thief has found the personal information, he or she will begin the process to create fraudulent accounts or misuse existing accounts of the victim.

- Pre-texting is another method of securing personal information on potential victims. Pretending to be a landlord, employer, or someone else with a valid reason to secure credit information, thieves will request your personal information from a credit bureau. They then use the information to create fraudulent credit cards or accounts.
- Steal information from your home. A thief can also get personal information from within your home. Obviously, a thief could break into your house and steal tax records or medical records with personal data on them. Most of us have little control over break-ins or theft by unknown persons. However, most people are not aware that a significant amount of identity theft is committed by an acquaintance of the victim. Almost 20 percent of identity theft is committed by someone known by the victim, such as a family member, friend, or co-worker.[16] Keeping key personal information in a secure location within your home or workplace will help prevent this potential problem.

Identity thieves can work individually or in groups in order to commit fraud. In both situations, ID thieves can steal and misuse the identities of many people at the same time. Some examples of just how successful some identity thieves are with these methods include:

- In one case, a ring of thieves working together stole the identities of 1,500 people. They created accounts and credit cards at 76 different banks and defrauded those banks of an estimated $1.6 million.[17]
- In another case, one Orange County, California man posed as an apartment manager and used fake residences and fraudulent information to create 60 to 80 identities.[18]

Financial Implications of Identity Theft

The financial implications are not as severe for the victims of identity theft as they are for the businesses that are defrauded out of merchandise or funds. The good news is that consumers are not responsible for the majority of the monetary damage caused by the thieves. If credit cards are stolen, federal law limits the consumer's loss to $50 per credit card. Many credit card companies go even further and do not hold consumers responsible for any loss after the credit card is reported stolen. ATM cards are a little more troublesome. If an ATM card is stolen, the consumer is responsible for $50 if the ATM card is reported stolen within two days. If it is not reported within two days, the consumer is responsible for $500. If the consumer fails to notify the bank within 60 days, the consumer is responsible for $50 and whatever charges or withdrawals occurred after 60 days but before the bank is notified.[19] In this situation, a consumer could have his or her entire bank account emptied by someone who has taken his or her ATM card and figured out how to access it. Consumers must pay close attention to their ATM card and the card statements, notifying the bank if they determine someone is accessing it illegally.

A checking account debit card can be even more of a problem as it doesn't require a Personal Identification Number (PIN) like an ATM card does. For this reason, use of a debit card by a thief can be more troublesome than the theft of an ATM.[20] In either case, theft of an ATM card or debit card can result in significant financial loss to the consumer as the thief can drain funds from the consumer's bank accounts.

Other types of ID theft can result in the creation of fraudulent loans, leases, purchases, and contracts being made. Fortunately, consumers are not responsible for the financial obligations created by these illegal activities. This is the "good news" but this is just part of the problem. The more costly problem is how identity theft affects your reputation and your credit record. Damage to the identity and credit record of the consumer can take hours of effort and substantial sums of money to repair.

The Real Cost of Identity Theft or "The Bad News"

In short, the "bad news" is that identity theft, although not financially devastating, can create havoc in your life and cause problems for consumers that cost more in lost time and effort than any financial loss they might suffer. Once a thief has stolen and misused a consumer's name, the consumer's credit score is affected. The thief opens credit card and bank accounts, makes purchases, but makes no payments on the bills created by his or her actions. When companies attempt to collect on these bills, the credit trail leads back to the consumer. The consumer is then forced to spend many hours trying to clear up his or her credit by identifying the fraudulent charges and getting them removed from his or her credit record. This sets up a chain of events that requires the consumer to spend many hours working to correct the damage created by the theft of his or her identity. Some of the more time-consuming and costly efforts include:

1. Clearing your name and credit—separating valid charges and bills from fraudulent ones.
2. Proving "who" you are—there are now "two" of you.
3. Responding to credit complaints—it takes many hours of time and many dollars in legal fees to respond to collection agencies and banks that pursue the consumer for bills created by the imposter. In the case of John Stephens, mentioned previously, it took him three years and $6,000 to clear his name.[21] Tracey Thomas, a

Continued on page 8

Identity Theft: Modern Problem, Modern Solutions: Part I

Continued from page 7

computer programmer in San Francisco, spent only $500 in legal fees to clear her name when someone stole her identity. But she had to use 400 hours of vacation time to clear her name because of fraudulent credit cards, leases, utilities, and cell phone accounts that were set up by the thief who stole her name.[22]

Identity theft does more than force consumers to spend time and effort to clear up their credit records. While consumers are attempting to clear their names, the negative activity on their credit report can prevent them from getting additional credit or securing loans. Many consumers have been denied loans for mortgages or to buy vacation homes because of bad credit ratings as a result of identity theft. Tracey Thomas was denied a loan to buy her first home because of the impact the identity theft had on her credit record.[23] In some cases, identity theft could even put a consumer in jail. Beth Givens, the director of the Privacy Rights Clearinghouse, states that if the identity thief commits a crime and uses the victim's name in that crime, an innocent person could end up going to jail. Stopped for a minor traffic citation, a check of open arrest warrants might land the consumer in jail because of actions by the identity thief.[24] In other cases, individuals have been denied jobs because of identity theft. According to the Federal Deposit Insurance Corporation, a department store clerk whose identity was assumed by a shoplifter, spent years looking for a job in the retail industry but was denied job opportunities because of the actions of the shoplifter, using her name.[25]

To add to the problem, many people do not become aware of the misuse of their name for several months or even years after the theft began. The Federal Trade Commission estimates that the average person is not aware of identity theft for 14 months after it starts.[26] This long period allows the perpetrator to do a lot of things before the victim can stop the fraudulent activities and begin the process to repair the damage. Once a victim becomes aware of the problem, it can take years to clean it up. Beth Givens indicates that it can take from six months to two years for someone to clear his or her record.[27] Some victims mentioned in this article indicated that it took them as long as three years to clear their records.

So, although identity theft may not result in much of a direct financial loss to a victim, the time and money needed to stop the fraudulent activities and repair one's credit record may well exceed the financial loss a victim might incur. Besides the amount of time and money needed to correct one's credit report, it requires time off from work and reduces the victim's income. The "hassle" factor of ID theft does have a significant financial tag on it as well. ■

Endnotes

1. Greenspan, Robyn; "The Big Picture," Cyberatlas.internet.com, November, 2001, p. 1.
2. Noack, David; "Identity Theft Thrives in Cyberspace," APBNews.com, March 8, 2000, p. 2.
3. Shakespeare, William, *Othello,* Act iii, Scene 3.
4. Department of Justice; "What Are Identity Theft and Fraud," USDOJ.gov, June 5, 2000, p. 1.
5. Barry, Patricia; "Thieves Get Rich Quick by Stealing Your Identity," *AARP Bulletin,* Nov. 1999, p. 1.
6. Lemos, Robert; "Identity Theft a Big Business," ZDNET.net, April 15, 1998, p. 1.
7. Ibid; "Identity Theft . . . " p. 2.
8. Panko, Ron; "Identity Indemnity," *Best's Review,* March 2002, p. 55.
9. Collins, Jeff; "Ring Accused of ID Thefts Amounts to $1.6 Million," *Orange County Register,* June 20, 2001, p. 1.
10. Associated Press; "ID, Credit Fraud Rising, Report Says," *Orange County Register,* Business Section, March 9, 2002, p. 3.
11. Cleaves, Joanne; "ID Theft Is a Growing Problem," *Friendly Exchange Magazine,* Spring 2002, p. 15.
12. Federal Trade Commission; "Identity Theft Complaint Data," *FTC Publication,* January 2001, p. 2.
13. *USA Today;* "Radical Solutions Eyed in Net Identity Theft Battle," USAtoday.com, June 19, 2001, p. 1.
14. Singletary, Michelle; "What's the Top Consumer Complaint? Identity Theft," SeattleP-I.com, February 5, 2001, p. 1.
15. *USA Today;* "Radical Solutions Eyed in Net Identity Theft Battle," USAtoday.com, June 19, 2001, p. 1.
16. Federal Trade Commission; "Identity Theft Complaint Data," *FTC Publication,* January 2001, p. 4.
17. Collins, Jeff; "Ring Accused of ID Thefts Amounts to $1.6 Million," *Orange County Register,* June 20, 2001, p. 1.
18. Padilla, Marie; "Anaheim Man Held in Identity Theft," *Orange County Register,* Local Section, April 14, 2002, p. 1.
19. Federal Deposit Insurance Corporation; "A Crook Has Drained Your Account, Who Pays?" *FDIC Consumer News,* Spring 1998, p. 1.
20. Ibid, "A Crook . . . ", p. 1.
21. Barry, Patricia; "Thieves Get Rich Quick by Stealing Your Identity," *AARP Bulletin,* Nov. 1999, p. 1.
22. Cleaves, Joanne; "ID Theft Is a Growing Problem," *Friendly Exchange Magazine,* Spring 2002, p. 15.
23. Ibid, "ID Theft Is a Growing Problem," p. 15.
24. Panko, Ron, "Identity Indemnity," *Best's Review,* March 2002, p. 58.
25. Federal Deposit Insurance Corporation, "When a Criminal's Cover Is Your Identity," *FDIC Consumer News,* June 2000, p. 1.
26. Federal Trade Commission; "Identity Theft Complaint Data," *FTC Publication,* January 2001, p. 4.
27. Lazarony, Lucy, "Identity Theft Insurance Is Available, But Do You Really Need It?" Bankrate.com, March 15, 2000, p. 2.

What's in IT for Me?

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

Have you surfed the IT Section web site lately? If not, take a few minutes to peruse the wealth of resources about technology, managing information, and business strategy. You'll find the following benefits for IT Section members:

- Contact information for your IT Section leaders, so you can voice your ideas and ask questions.
- Web links to many insurance and technology-related web sites and white papers.
- Links to free webcasts.
- Event calendar that highlights upcoming information technology events scheduled around the country.
- User tips and trends.
- Latest information technology news and links.
- Members-only benefits such as access to online copies of the quarterly *Cutting Edge* newsletter and archived research articles; special members-only promotions and contests: Powerpoint presentations and seminar recaps from IT-sponsored symposia.

Make the most of your IT Section membership by taking advantage of these resources and letting us know what else you'd like to see on the web site. We're listening to you!

You may contact the webmaster at cpcu-infotech-section@earthlink.net. ■

http://infotech.cpcusociety.org

Information Technology Section Committee Spotlight—Glen R. Schmidt, CPCU, CLU, FLMI

■ **Glen R. Schmidt, CPCU, CLU, FLMI**
State Farm Group
Bloomington, IL

Glen R. Schmidt, CPCU, CLU, FLMI, began his insurance career in the Columbia, MO regional office with State Farm Insurance in 1969, following a three-year commitment in the United States Army. Glen graduated from Central Missouri State University with a bachelor's degree in business administration. After spending several years in auto and fire underwriting positions, he moved to Bloomington, IL, in a data processing function. Glen is currently a business analyst with State Farm in its Systems Department with primary responsibility in the system design, development, and procedural writing for fire operations.

He has served on numerous CPCU Society chapter committees at the local level and has been involved at the national level for more than 10 years. Glen was the chairman of the Candidate Recruitment and Development Committee and recently completed a three-year term as chairman of the Total Quality Section Committee.

He is married to Ginny, who recently retired from State Farm, and they have two children. His hobbies include gardening and antiquing, and looking forward to becoming a first-time grandpa. ■

IIABA Launches Big "I" Markets Version 1.2

According to a news release dated March 26, 2004, Big "I" Advantage, the products and services subsidiary of the Independent Insurance Agents & Brokers of America (IIABA), has released an upgraded version of the Big "I" Markets software to its more than 3,500 participating agencies (including 8,000 registered users). The new version, 1.2, offers users more secure technology, easier navigation, and an increased capacity to take on new products.

Big "I" Markets provide access to specialty/niche coverages, program business, and hard-to-find markets exclusively for IIABA members. Using proprietary IIABA technology and IIABA's nationally licensed, wholly owned agency—IIAA Agency Administrative Services—IIABA members gain access to available coverage, terms and conditions, applications, a quote request platform, and policy forms, and electronic brochures are efficiently conveyed to and from IIABA agents and product providers.

IIABA launched Big "I" Markets in 1998 based on Microsoft's then brand-new data and permissions management tool, Active Directory (AD). Big "I" Markets Version 1.2 builds on that platform using Windows Server 2003 updates for AD. Big "I" Markets President, Paul Buse, stated, "(b)y using IIABA's AD infrastructure, we can control what product or coverage members see based on their license with us and what is available in their states." Version 1.2 of the Big "I" Markets brings with it new products from Balboa, Fireman's Fund, and National Interstate. These new products are added to those already available from Atlantic Mutual, Chubb, The Hartford, Selective, The St. Paul, and others.

The new, enhanced user interface of Big "I" Markets is built in object-oriented JAVA while the application data collection and exchange were designed embracing Extensible Markup Language (XML) standards. In discussing the new Version 1.2, Buse stated, "(w)e have all kinds of technology. . . . Perhaps the most important aspect of Big 'I' Markets Version 1.2 is that it helps bring to the marketplace a combined Big 'I' member distribution force for specialty products." ■

SERFF Use Tripled in 2003 Over 2002, Achieves First 10,000-Filing Month in 2004

We have an update to follow the NAIC SERFFing article from the previous issue of *Cutting Edge*. In a news release dated March 15, 2004, it was announced that SERFF use has tripled in 2003 over 2002. During 2003, more than 76,000 filings were channeled through SERFF, which is nearly a 300 percent increase over filings made in 2002. The NAIC has estimated that between 140,000 and 150,000 filings will be made in 2004.

SERFF was first introduced in 1998 by the National Association of Insurance Commissioners (NAIC). Now, 49 states, the District of Columbia, and Puerto Rico are capable of accepting filings through SERFF. According to the NAIC, by the end of 2003, 50 states accepted property and casualty filings, 48 states accepted life insurance filings, and 41 states accepted health insurance filings.

NAIC President Enrst Csiszar summed up the benefits of SERFF in stating, "[p]art of our regulatory modernization is to dramatically reduce the time and cost of rate and form filing regulatory compliance, and this is evidence that we are achieving that goal . . . SERFF is simply more cost-effective than antiquated filing methods and it allows information to become accessible much more quickly."

Currently, more than 1,200 insurance companies are licensed to use SERFF and have found that in using SERFF, they experience only a 23-day turnaround in the filing review cycle. ■

New ACORD-ILOG Survey Reveals Insurance Industry Response to Compliance Challenges

Editor's note: The following information was taken from an ACORD-ILOG press release dated April 6, 2004.

According to survey results released by ILOG® (Nasdaq: ILOG; Euronext: ILO, ISIN: FR0004042364) and ACORD, the Association for Cooperative Operations Research and Development, the insurance industry's response to fast-changing regulatory and corporate governance business demands is characterized by a primary reliance on manual processes and ad-hoc measures. Although specially-appointed compliance officers generally have been assigned to manage the impact of regulatory demands, the survey revealed the industry is failing to fully embrace the high business value of information technology when addressing regulatory requirements such as HIPAA and corporate governance demands driven by mandates such as the Sarbanes-Oxley Act.

The survey, conducted over the course of two months from December 2003 to January 2004, asked representatives from property and casualty, life insurance, and reinsurance companies to consider how effectively their organizations are addressing compliance mandates, and to report on the role of technology as it pertains to managing compliance regulations.

The study clearly demonstrates challenges for insurance companies seeking to streamline and automate core business processes to help manage the impact of compliance, including: a reactive rather than proactive culture (410); inflexible technology infrastructures that do not easily support new and changing regulations (28); and a continued reliance on manual and paper-based processes (140). Key findings of the study are as follows:

- Human Involvement Drives Compliance Management: While 830 of insurance companies surveyed have appointed compliance officers to direct their company's response to the impact of regulatory compliance, only 17 directly involve IT while implementing guidelines to manage and minimize the impact of regulatory compliance.
- Ad-Hoc Measures Characterize Response: Although the majority of insurance company representatives surveyed (830) believe their organization is effectively managing the obligations imposed by the new compliance regulations, 42 percent of the companies surveyed address compliance regulation issues on an ad-hoc, reactive basis, an indication the industry is failing to put process-automating technologies in place to manage core business processes across lines of business.
- Limited Technology Implementations Planned: One quarter (2,561) of the companies surveyed planned to implement an enterprise-wide strategy to address the obligations associated with regulatory compliance and related changes, while an equal number of respondents (250) plan to implement a solution that allows monitoring for distinct lines of business.

"This survey reveals there is a clearly defined line between companies who are embracing IT to address compliance regulations head on and those who are not," said Kate Ciravolo, CPCU, vice president and counsel, government affairs for ACORD. "While we're pleased that the industry is taking the first step by appointing compliance officers to manage the process, those companies that fail to leverage this opportunity to automate core business processes and standardize across their enterprises are likely to fall victim to increasingly complex federal and state regulations."

The two top technology solutions respondents reported considering or using to manage compliance include business process management (BPM) and business rules management systems (BRMS)—38 and 21 percent, respectively. These two complementary technologies are key drivers helping businesses automate and streamline core business processes.

A report from Giga Research, a wholly owned subsidiary of Forrester Research, "Market Overview 2003: Rules Platforms—Standing at the Threshold of Mainstream IT," notes that business rules platforms are entering the IT mainstream. Gartner further notes that, "Every U.S. business must comply with thousands of federal business regulations. Process management technologies and business rules engines can help companies understand new rules and enforce compliance policy." (Source: Process Management Technology Makes Compliance Easier, Debra Logan; May 2003).

Need to Align Perception and Reality Identified

In an indication that the industry response to compliance is subject to the redundancy and errors associated with manually driven processes, most companies surveyed continue to rely on human-directed—rather than automated—solutions, and the majority have yet to deploy available technology solutions in order to align business objectives with IT.

More than one-third (380) of insurance company representatives agreed that the primary objective to managing the impact of compliance through IT is to improve operational efficiency in core business processes by utilizing, for instance, technology solutions that increase automation. Yet, while the majority of the organizations surveyed have designated a compliance officer or team to ensure they are meeting compliance regulations, less than one-quarter of the companies surveyed (21 percent) leverage their IT department in conjunction with the compliance officer.

For more details, please visit www.ilog.com, or contact them at (800) FOR-ILOG. ■

The CPCU Society Presents . . .

"Reach for the Stars!"

60th Annual Meeting and Seminars
Los Angeles, CA, October 23-26, 2004

Join other CPCUs, new designees, and industry VIPs in Los Angeles for the best in education, networking, and leadership the property and casualty insurance industry has to offer—and to "Reach for the Stars!"

- Focus your continuing education on the skills—and CE credits—you need to succeed, with more than 20 Property and Casualty Insurance Track seminars to choose from.
- Learn the communication, management, planning, and organizational skills needed to advance your career through more than 20 Leadership and Career Development Track seminars.
- Meet CPCU Society members, colleagues, and industry leaders who can influence your success at an exciting variety of Special Events.
- Open your eyes, your heart, and your mind to a radical redefinition of the leadership skills you and your organization need with 2004 Keynote Speaker Tom Peters, renowned business thinker, speaker, and best-selling author.
- Celebrate 60 years of CPCU Society success at special 60th anniversary celebratory and recognition events throughout the Annual Meeting.

Register Today!

It's the professional development event of the year. For the latest information about this year's meeting, to register online, or to download the registration form, visit the CPCU Society web site, www.cpcusociety.org. If you have any questions or if you'd like to request a registration form, contact the Member Resource Center at (800) 932-CPCU, option 5, or e-mail us at membercenter@cpcusociety.org.

Insurers Nearsighted on Their Decisions According to Sapiens Survey

Editor's note: The following information was taken from a Sapiens press release dated March 15, 2004.

Sapiens International Corporation (NASDAQ and TASE:SPNS) announced results of its survey of U.S.-based senior insurance executives on industry IT trends conducted at the ISOTech tradeshow in Anaheim, California, in late 2003. The survey uncovered an industry inclination toward short-term solutions and quick fixes that could harm companies downstream.

According to the survey, a flat or reduced IT budget ranked high on insurance executives' list of short-term market impacts through 2004 and less than half of respondents predicted IT budget increases through 2006.

Asked to rank the greatest market impact on corporate strategy in the short term, 22 percent pointed to focus on internal IT efficiency and cost containment, 17 percent internal infrastructure focus versus external, and 12 percent legacy systems modernization. The short-term strategies are paving the way for anticipated medium-term activities through 2006, including extending distribution channels to meet new demand (15 percent), rationalizing supported platforms (14 percent), and moving to data and development standards (14 percent).

Survey participants also identified the need for agile systems to support changing business conditions (17 percent) as the most significant automation driver in the near-term in order to meet complex market challenges and the need to control operational costs. Needs driving automation were:

- Agile Systems to Support Changing Business Conditions . . .17%
- Minimize Time and Cost to Maintain Inflexible Legacy Environments 13%
- Better Information and Service to/from Distribution Channels . . .11%
- Automate Manual or Partially Automate Processes 11%
- Better Information to Support Customer and Business Exposure Management . .11%
- Achieve ROI for the Business or Line of Business 9%
- Standardize Development Environments and In-House Skill Requirements 8%
- Integrated Systems and Services for Quicker Regulatory Compliance 8%
- Better Business Contingency and Recovery Support 7%
- Separate, Document, and Validate Core Business Logic 5%

Illustrating the same tactical outlook, top critical IT success factors cited by respondents were as follows:

- Better Underwriting for Improved Profitability 26%
- Integrating Systems to Reduce Time and Cost 24%
- Operating in Real Time with Distributors 21%
- Enabling Rapid Response to Markets and Regulators 8%
- Increased Visibility of Data and Systems to Streamline Processes . .7%

Integrity issues such as managing IT-based risks and increased traceability of business transactions received lower weight as critical, short-term IT success factors, 4 percent and 6 percent, respectively.

To help insurers achieve internal efficiency goals and keep costs in line, IT outsourcing is either underway (36 percent) or under consideration (20 percent) in more than half the respondents' organizations, and business process outsourcing (BPO) is rated as a key consideration through 2004.

Despite continued interest in IT outsourcing and cost containment, 50 percent of respondents indicated their organizations' plan to build new applications through 2004 and an additional 32 percent stated they would build with a vendor. A significant decrease in pure in-house development to 26 percent is predicted by 2006, but is slightly offset by an increase in respondents planning to build with a vendor (from 32 to 45 percent). An increased number of insurers also anticipate purchasing packaged applications during the next three years (from 14 to 23 percent), while planned use of outsourced options remains largely constant.

"Clearly, a tactical business focus continues to drive insurance organizations," said Judy Johnson, vice president of insurance strategies for Sapiens Americas. "However, a short-term focus could mean duplication of legacy issues in newer systems. Insurers cannot obtain the medium-term results they desire without changing the way they manage IT. A short-term focus that fails to account for escalating business and IT integrity issues could find insurers facing the same health and reputation challenges as some former household name organizations."

For more information or to obtain a copy of the survey, please contact Sapiens vice president Judy Johnson at judy.j@sapiens.com. ■

2003 Annual Meeting Seminar

Leveraging Third-Party Data to Improve Claims Management

Patricia L. Saporito, CPCU, discussed the importance of claims-related data, and stressed the importance of a single data repository.

In this IT Section-sponsored session, section committee chairman Patricia L. Saporito, CPCU, addressed the analytic perspective, and G. Victor Guyan of Accenture Insurance Solution Group addressed operational aspects of using external data to improve claims costs.

Saporito emphasized the importance of claims and claims-related data stating that for every dollar of premium, claims adjusting expense, and loss payments, represent more than 80 percent of the dollar; the insurance equivalent of "cost of goods" sold. She discussed the growth of data—total data will quadruple in the next two years, and the challenges that managers face using it—including the sheer volume of data, data quality issues, the increase in the number of daily decisions, and less time to make them. She prescribed harnessing external data to augment internal data, aggregating and organizing it, and making it accessible to claims professionals with more sophisticated analytics in day-to-day operations. She stressed the importance of creating a single data repository with different business views to meet the needs of various business users as claims data is used not just by claims but by actuarial, underwriting, and loss control. She ended by providing examples of best practices in medical management, salvage, subrogation, and catastrophe reinsurance recoveries using prescription, warranty, weather, and other types of external data.

Guyan stated that insurance is an information business—that it's our currency for underwriting, pricing, and claims management. He discussed operational opportunities including fraud detection, medical management and bodily injury, and disability evaluation. He further discussed the use of location data and geographic information systems. He also addressed issues including data quality, timeliness of the data, detail level of the data, data history, and the changes in business processes needed. He stressed lessons learned—this is a process, not just a data access issue; you cannot build a claims process by assembling a collage of data sources and providers. Each insurer needs to organize its own business process and internal systems to take advantage of the data and outside services available.

G. Victor Guyan shared his views about insurance being an information business, and stated how important data is to various operational processes.

For more information, contact patricia.saporito@ncr.com or g.victor.guyan@accenture.com.

See page 16 for more information about IT Section-sponsored seminars at the 2004 Annual Meeting and Seminars.

Security and Access Controls in the Workplace: Proximity Cards and Beyond

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

Lynn M. Davenport, CPCU, AIC, AIM, AIS, AIT, graduated with a B.A. in psychology from St. Mary's College, Notre Dame, IN, in 1989, and began her career with State Farm Insurance Cos. as a claim representative. She previously trained new fire claim employees and supervised the subrogation department. For eight years, she managed a team of innovators who supported the claims technology and recommended efficiency processes in Colorado, Utah, and Wyoming. Currently, Davenport is responsible for implementing new claims technology and processes throughout six states over 18 months.

Davenport earned her CPCU designation in 1999 and is active in the Colorado Chapter as web site manager in addition her work with the IT Section. She has completed AIC, AIM, AIS, AIT, and is currently pursuing an M.B.A. through Walden University. In her spare time, she enjoys traveling with her husband and two children, skiing, and shopping.

Workplace security has become a growing concern for many employers and employees. After September 11, many companies implemented tighter controls for access to their buildings and offices. One way that employers can strengthen security is through "smart" electronic employee ID badges or proximity cards. Proximity cards were originally developed for "validation and privilege management" purposes but technology continues to expand the capabilities of monitoring employees through electronic ID cards (CoreStreet, 2002).

Proximity cards do much more than allowing employees to walk through the front door of a company's building (Hanson, 2002). These cards can serve multiple purposes for identification control, access control, and activity monitoring:

- Photo identification of the employee.
- Electronic key access to buildings and secured rooms within buildings.
- Customization of access: the cards can be programmed to grant 24/7 access to all company sites, or restrict access to the single physical building where the employee is assigned and limit access to the employee's assigned shift.
- When employees use their proximity card to access a building, the date, time, location, and employee information are captured electronically. This allows the company to track when and where the employee is going while on the employer's property.
- Cards can be expanded to include smart card technology, where electronic funds could be transferred and company financial transactions by employees could be monitored. Technology is available to load the employee cards with e-cash so they can pay for their food at the company cafeteria without having to exchange physical cash (Sigma Science Corporation, n.d.) or pay for a can of soda at the vending machine (Hanson, 2002). This would allow companies to monitor the financial transactions of employees at work.
- Also, more personal information can be stored on the chip in the smart card, which could potentially enable employers to track workers' exact locations in the building, log on to their computer and track their activities on the Internet while they're wearing the badge, maintain attendance and health information records (Hanson, 2002), and on and on. The possibilities are endless.
- Some companies are expanding to biometrics technology in their employee identification efforts, which provide even greater control. Although someone could counterfeit an employee photo ID badge, a fingerprint or pupil analysis is much more difficult to present as a fake. Biometrics are the next generation of access control technologies.
- When an employee is terminated, the card should be immediately revoked. If this is not possible, it should be reprogrammed to exclude access to any company buildings. If it's a smart card, transaction capability should also be revoked.

References

CoreStreet, Ltd. (2002). ID cards. Retrieved October 5, 2003, from Google at http://216.239.41.104/search?q=cache:FInrkSNMhUwJ:www.corestreet.com/solutions/CoreStreetIDCards.pdf+electronic+employee+ID+cards&hl=en&ie=UTF-8.

Hanson, J. (2002, June). Access, unlimited [electronic version]. *CSO Magazine.* Retrieved October 5, 2003, from http://www.csoonline.com/read/060103/toolbox_1394.html.

Sigma Science Corporation. (n.d.) Electronic payment strategies. Retrieved October 5, 2003, from http://www.sigmascience.com/electronic.html.

The Information Technology Section Is Proud to Announce that It Will Sponsor Two Informative Seminars at the 2004 Annual Meeting and Seminars in Los Angeles!

Agency-Company Automation and Technology Compatibility

Sunday, October 24, 1 - 3 p.m.

What You Will Learn

More and more, greater internal and external demands are placed on improving independent agencies' operations and effectiveness. To minimize the expense of automation improvements, greater cooperation and coordination is needed between the independent agents and the companies they represent to ensure automation compatibility. This seminar explores these issues with the intent of companies and agencies making the optimum automation decisions by balancing both agency and company needs and expense issues.

Business Continuity Planning—An Information Technology Perspective

Monday, October 25, 2 - 4 p.m.

What You Will Learn

Disaster can strike at any moment—but you can learn how to cope with the worst. This three-part seminar will address the crucial issues of crisis management planning, emergency response and business resumption, and rebuilding your organization. Attendees will learn to recognize the exposures faced by an organization from an information technology and automation standpoint. This program will also address the need for pre-planning efforts to ensure the survival of an organization as well as an understanding of the steps to re-establish your data and/or technology environment following a disaster.

Register today at www.cpcusociety.org!

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 and GF Practices, Inc.
Phone (410) 366-3796
e-Mail: bobsiems@gfpractices.com

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

Sections Manager
John Kelly, CPCU, AIT
CPCU Society

Managing Editor
Michele A. Leps, AIT
CPCU Society

Production Editor/Design
Joan Satchell
CPCU Society

CPCU Society
PO Box 3009
Malvern, PA 19355-0709
(800) 932-2728
www.cpcusociety.org

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

Cutting Edge

IT

Volume 11 Number 2 June 2004

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

PRSRT STD
U.S. POSTAGE
PAID
BARTON & COONEY