

# ...CPS BULLETIN...

The Newsletter of CPS Actuaries and Computer Programming & Systems, Inc.

Volume 3, Issue 1

October 2002

## Introduction

This issue of **CPS Bulletin** focuses on privacy issues and the Internet. Our lead article describes how the Internet has, in some ways, reduced our privacy while simultaneously producing ways to counteract this unwelcome development. We discuss, in particular, Identity Theft, which occurs when someone assumes or takes over your identity (usually name and social security number) and uses it for negative purposes such as obtaining credit cards or even buying a house by taking out loans in your name.

Our second article discusses the fight against terrorism by outlining the requirements of the USA Patriot Act of 2001 and how it will affect fraternal benefit societies.

We have also provided an update on the progress of the 2001 CSO Table and the new Actuarial Opinion and Memorandum Regulation (AOMR). The AOMR, which will be adopted by a number of states during 2003, eliminates Section 7 actuarial opinions; therefore, all companies and fraternal will now be required to perform asset adequacy analysis when preparing the actuarial opinion.

We hope that you enjoy receiving this newsletter. If you have any comments or suggestions on how we can improve **CPS Bulletin**, please contact us by visiting our company web site at [www.cpsincorp.com](http://www.cpsincorp.com) ❖

## Privacy Protection and the Internet

Let's start with a little experiment. Type your name into any search engine (such as Google or Yahoo) and see how much information you can find about yourself on the Internet. Chances are that you might find some information about yourself, but not much. However, type your name into People Search on Yahoo.com and notice the advertisements that appear. You will be offered the services of businesses that gather information on bankruptcies, criminal history, background checks and a search of public records. Your medical records may also be available (despite legislation) to almost anyone.

How can so much information about you be available on the Internet? In the case of medical records, one reason may be that you signed "blanket waivers" or "general consent forms" when you obtained medical care. When you sign such a waiver, you allow the health care provider to release your medical information to insurance companies, government agencies and others.

Insurance companies usually require you to release your medical records before they will issue a policy. Medical information gathered by one insurance company may be shared with others through the Medical Information Bureau. Moreover, privacy letters from insurers often state something similar to the following: "When necessary or appropriate for your treatment or other related activities, we use nonpublic personal information internally, share it with our affiliates, and disclose it to health care providers, other insurers, third party administrators, vendors, consultants, government authorities, and their respective agents." In plain language, this says that your medical records may be shared with just about anybody the insurer wants to do business with – or with any government agency – without further consent or permission, unless you opt-out from the sharing of such information.

## INSIDE THIS ISSUE

- 1 Introduction
- 1 Privacy Protection and the Internet
- 3 Fraternal and the USA Patriot Act
- 4 Regulatory Update
- 4 Interest Rate Monitor
- 4 About CPS

See **Privacy Protection and the Internet** on page 2

Government agencies may request your medical records to verify claims made through Medicare, Social Security Disability and Workers' Compensation. Again, in these instances, your medical records may be shared with others.

Thus, the Internet has widened our exposure to the outside world. Some of the exposure is voluntary, such as when you publish something on the Internet or are included in an article about someone else. And some of it may be involuntary, such as when we provide credit card information to web vendors or even when we simply go surf the Internet.

We have discussed in previous newsletters the availability of elementary precautions (such as firewalls) to protect oneself against the invasion of privacy by spammers. In this article we wish to focus on more sinister problems, such as identity theft and the privacy of medical records

Identity theft is the fastest growing white-collar crime and it occurs when someone takes over your identity and uses it for negative purposes such as obtaining credit cards in your name. To be able to do this, the thief has to have significant information about you – the sort of data you supply each time you make a purchase over the Internet.

It should be immediately noted that it appears no less safe to provide such information via a secure, encrypted, "known" site on the Internet than letting an unknown supermarket clerk take an imprint of your credit card.

These are the steps that will help to protect your identity. Since identity theft cannot take place without accessing your credit information, this information is the key to prevention. First, visit some of the sites that deal with identity theft. The first places to start could be the government's site <http://www.consumer.gov/idtheft/> or sites run by non-profit groups, such as [www.privacyrights.org](http://www.privacyrights.org) and [www.idtheftcenter.org](http://www.idtheftcenter.org). The government site has a wealth of good information. For example, the site provides a sample "opt out" letter that can be sent to the major credit bureaus in order to request that your personal information not be shared with others.

The second step is to obtain a current snapshot of your

credit information. This is a very useful procedure to carry out periodically, regardless of whether one is wary of identity theft or not. This ensures that your data is as up-to-date and as error free as possible. You can then request the bureaus to correct any inaccurate data.

There are a number of Internet based services that can assist you once identity theft has taken place. These companies will work with you to take corrective action. These services may not do more than what an individual can do on his own, but they will help by providing the necessary forms and telephone numbers, and assist in gathering evidence against the perpetrator. They may even get on the phone when you deal with credit bureaus to facilitate the process of repairing any damage. Some companies include an insurance element as part of their fees; this will reimburse you for expenses incurred in rectifying the situation, such as legal fees and travel expenses that could amount to thousands of dollars.

There are other companies that will monitor your credit record for various indicators of possible fraud and weekly notification of any (suspicious) activity

We have not tested any of these services but some of the better-known companies in that field are [www.promiseplans.com](http://www.promiseplans.com), [www.privacyguard.com](http://www.privacyguard.com) and [www.identityfraud.com](http://www.identityfraud.com). The annual cost of membership in these plans varies by level of service and is between \$30 and \$125.

Currently, there are *no* comprehensive laws regarding medical records privacy. For medical records, you should attempt to protect yourself by making the release you sign for medical providers specific rather than general.

As with credit records, you can obtain a copy of the Medical Information Bureau records by sending \$9 to P.O. Box 105, Essex Station Boston, MA 02112 or calling (617) 426-3660. You can also obtain this information by visiting their web site at [www.mib.com](http://www.mib.com).

Finally, the Health Privacy Project of Georgetown University is a resource for public policy information on medical records confidentiality. Its web site ([www.healthprivacy.org](http://www.healthprivacy.org)) includes information on federal as well as state privacy regulations and legislation. ❖

---

## **Fraternal and the USA Patriot Act**

The USA Patriot Act of 2001, signed into law on October 26 2001, will drag fraternal into the fight against terrorism. This article will outline some of the more important items associated with the Act.

### **Why is it called the USA Patriot Act of 2001?**

Believe it or not, the USA Patriot Act is actually an acronym for the “**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism” Act.

### **Is this an entirely new Act?**

The USA Patriot Act makes numerous changes to the Bank Secrecy Act (BSA). The Patriot Act effectively drafts financial institutions into the war on terrorism. The BSA is one of the main federal laws requiring monitoring of financial information. The Patriot Act requires financial institutions to demonstrate greater vigilance in detecting and preventing money laundering activities.

### **What’s the definition of a “financial institution” under the Act?**

A financial institution is defined very broadly under the Act. Many of the entities defined as a financial institution are obvious, including banks, brokers or dealers registered with the SEC and insurance companies. However, the definition also includes some that are not so obvious, including fraternal benefit societies, pawnbrokers, dealers in precious metals, travel agencies, telegraph companies, companies involved in the sale of cars, the US Postal Service and persons involved in real estate closings.

### **Why are insurance companies and fraternal being considered as financial institutions?**

Federal law enforcement authorities have discovered that drug cartels have been hiding their illicit proceeds by purchasing life insurance contracts. The money-laundering scheme involves the purchase of several life insurance policies with cash surrender values. The policies are funded by narcotics proceeds that are forwarded to the insurance companies by third parties from around the world. Although the cash surrender value is far less than the amount invested, the beneficiaries liquidate the policies for their cash

surrender value. Although the beneficiaries suffer a financial loss, the funds received (in the form of insurance proceeds) are effectively laundered.

### **What are the duties of agents of insurers with regard to the Act?**

Currently, the Act does not require agents to independently establish an anti-money laundering program. However, because of their direct contact with customers, insurance agents are in a unique position to observe the kind of activity that may be indicative of money laundering. An agent may be able to detect suspicious activity, such as the purchase of an annuity policy by customers who express little or no interest in the details of the product, such as surrender charges. The agent would know more about the customer in this case than the insurer, especially when policies are purchased with very little underwriting.

### **What must an insurer do to comply with the Act?**

Each insurer must develop and implement an anti-money laundering program to prevent itself from being used to facilitate money laundering activities or the financing of terrorist activities. The program must be in writing and approved by management.

### **What are the requirements of an anti-money laundering program?**

There are four requirements for an anti-money laundering program:

- (1)** Develop internal policies, procedures and controls for the anti-money laundering program.
- (2)** Designate a compliance officer to be responsible for administering the anti-money laundering program. This may be one person or a committee.
- (3)** Provide for education and training of appropriate personnel. The employees must be trained so that “red flags” associated with existing or potential customers can be identified.
- (4)** Periodically provide independent testing of the program to ensure that it complies with the Act and that the program functions as designed. This audit may be performed by an outside

See **Fraternal and the Patriot Act** on page 4

consultant or by an employee of the company, so long as that employee is not the compliance officer or involved with administering the program.

**What is the role of the compliance officer?**

The compliance officer should be knowledgeable regarding the BSA requirements and money laundering issues and risks. The officer should have the authority to develop and enforce appropriate policies and procedures. The officer must ensure that (1) the program is being implemented effectively, (2) the program is updated as necessary, and (3) employees are trained with regard to the program.

**By what date must a fraternal be in compliance with the Act?**

The Act was adopted on October 26, 2001. However, the Patriot Act will not apply to fraternal benefit societies until October 26, 2002. If you would like assistance in developing an anti-money laundering program, please contact CPS and we can assist you in this regard. ❖

**Interest Rate Monitor**

The following are some key interest rate benchmarks:

Benchmark	Current	3 Months Ago	1 Year Ago
Fed Funds	1.75%	1.75%	2.50%
Prime Rate	4.75%	4.75%	5.50%
30 yr mortg	5.72%	6.08%	6.17%

Source: [www.bloomberg.com](http://www.bloomberg.com) as of October 9, 2002.

**About CPS**

*CPS Actuaries and Computer Programming & Systems, Inc.*

CPS is an independent company with over 35 years of service to our clients. We offer a wide range of computer and actuarial services. For information regarding our services, please call us at **203-324-9203**, or visit our web site at [www.cpsincorp.com](http://www.cpsincorp.com) ❖

**CPS, Inc.**  
**1014 Hope Street**  
**Stamford, CT 06907**

**Regulatory Update**

**2001 CSO Mortality Table**

The Table has received the go-ahead and the NAIC is prepared to accept it at their meeting in December. This means that the Table will probably be available beginning in 2003 in some states. All companies must adopt the Table by January 1, 2009. Any company that chooses to use the Table will have to provide an actuarial opinion that is based on an asset adequacy analysis. The adoption of this Table means that virtually all life insurance products will need to be re-priced and re-filed over the next few years.

In our last issue of **CPS Bulletin**, we indicated that some companies would be required to file mortality data with the Society of Actuaries as part of the adoption of the new Table. However, this requirement has been eliminated and therefore companies will not have to submit their mortality data.

**Actuarial Opinion and Memorandum Regulation (AOMR)**

After some serious discussions among industry representatives and regulators over the past few years, a new AOMR was finally adopted by the NAIC. According to the new AOMR, all companies, regardless of asset size and solvency strength, must now perform a Section 8 actuarial opinion. A Section 8 opinion will require an actuarial opinion that is based on asset adequacy analysis. Previously, most small fraternal could file a Section 7 opinion that exempted them from having to perform such an analysis. Early indications are that states will permit a Section 7 opinion with the December 31, 2002 annual statement. However, about 20 states are prepared to require a Section 8 actuarial opinion beginning with the December 31, 2003 annual statement. The remaining states are expected to pass the new AOMR in 2004.

CPS is prepared to handle the asset adequacy needs of small-to-medium sized fraternal in a timely and economical manner. Please contact us if you would like to discuss the benefits and costs of such an analysis for your organization. ❖