



# THE FILE ROOM

## IN THIS ISSUE:

**Imaging:  
In-House  
Versus  
Outsourcing**

**To Buy or  
Not To Buy:  
Identity Thief  
Spawns New  
Products and  
Services To Help  
Minimize Risk**

**The Benefits of  
Document  
Imaging**

**COMING  
SOON:**

**Training  
Employees  
in Record  
Management**

**Phone  
(314) 209-0600  
Fax  
(314) 209-0120**

## **IMAGING: IN-HOUSE VERSUS OUTSOURCING**

Are you ready to scan it all and throw out the boxes of paper records? Well...not so fast. Are you going to electronically scan a document so that it is easy to access and use in your day-to-day business process, such as an invoice? Or are you going to scan certain documents onto microfilm to protect them as vital information that can be stored long term? Are you going to do the scanning yourself in house, or outsource the process to an imaging facility?

There is an excellent free source on line that clearly lays out the pros and cons of each approach in great detail. It is called the Digital Imaging Tutorial from the Cornell University Library ([www.library.cornell.edu/preservation/tutorial/management/management-03.html](http://www.library.cornell.edu/preservation/tutorial/management/management-03.html)) and here are some of the points it makes.

### **If you do it yourself, consider these necessities.**

Some of the tasks that will have to be staffed include: identification, selection, preparation, digitization, metadata creation, quality control, cataloging, data control, systems support, and management. Plus maintenance of the database and web delivery system. Also, there will be start-up training as well as ongoing training as new systems or new staff members are added later.

There will be a need for office space that is dedicated to the scanning function, with 75 to 150



square feet per person, adequate workspace, tables and shelves. The facility must also have phone and data lines, LAN connection, and protection for uninterrupted power supply. Because scanning equipment and lights can raise temperatures, proper HVAC, lighting and air filtration are important. Hardware will include scanners, monitors, workstations, peripherals, servers and printers, plus the software to make all this work, and other supplies as well.

The advantages to having your own operation are that you have control over all the imaging functions; there is security for and proper handling of all materials; you maintain quality control; and you learn by doing. The disadvantages are that a large amount of money must be spent on getting the operation up and going instead of spending it on products (scanned documents); the facility may necessarily be limited as to production capabilities; and the equipment will likely work its way into obsolescence.

## **DID YOU KNOW??**

- 90% of corporate memory exists on paper
- Of all the pages that get handled each day in the average office, 90% are merely shuffled.
- The average document gets copied 19 times.
- Companies spend \$20 in labor to file a document, \$120 in labor to find a misfiled document, and \$220 in labor to reproduce a lost document.
- 7.5% of all documents get lost, 3% of the remainder get misfiled.
- Professionals spend 5-15% of their time reading information, but up to 50% looking for it.
- There are over 4 trillion paper documents in the U.S. alone – growing at a rate of 22% per year.

*Source: Coopers & Lybrand*

## **Would it be better to outsource the scanning function?**

Quite possibly, yes. However, there will still be certain parts of the digitization chain that will need to be supported by your organization such as in-house inspection. There are some advantages to outsourcing such as the following.

Your organization pays for delivered product at a cost-per-image which makes it easier to plan and budget for a project or ongoing need. Costs usually are lower than in-house costs but can vary based on kind of project and geographic area. A contractor can handle larger volume, and can offer other services such as encoding, metadata creation, derivative creation, storing and backup, and database creation. Plus the vendor has the costs for staff, training and equipment.

The picture is not totally rosy, however. Your organization is put at arm's length by the fact that the imaging is done offsite or even off shore. There may be problems with security and transportation of your materials. If communication breaks down concerning production or quality control issues, there are few if any best practices to help define or negotiate good service.

To begin to get some specifics on scanning, consider reading these documents which are available on line from the Library of Congress (<http://memory.loc.gov/ammen/about/techIn.html>). One is titled "Technical Standards for Digital Conversion of Text and Graphic Materials" and another is "Conversion Specifications for Contracted Scanning Services."

## **That said, there are still good reasons to consider outsourcing your scanning.**

Some of them are set forth by the Document Scanning Companies of America (DSCA), a consortium with member companies in each state ([www.docuscanamerica.com](http://www.docuscanamerica.com)). The main premise of this group is that there are many laws on the books now that mandate protection for and limited access to certain confidential records.

HIPAA, the Health Insurance Portability and Accountability Act, includes privacy rules governing patient health records saying that "a covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information."

Gramm Leach Bliley (GLB) is a federal law with broad standards designed to compel financial institutions to "respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information," and to provide protection against "unauthorized access to or use of such records...resulting in substantial harm or inconvenience to any customer."

FACTA, the Fair and Accurate Credit Transaction Act of 2003, has provisions to combat consumer fraud and identity theft involving personal information of employees and customers including rules for eventual destruction of such documents.

According to DSCA, the answer is to scan personal records onto disks and restrict access to these electronic files instead of having paper records which can be viewed by many people.

Putting aside the privacy issue, there are other kinds of documents that could be indexed and scanned and made available on line for quick access. First to mind is the area of customer service where accessible records enable employees to give quick and correct answers to questions instead of having to go through paper files and get back to a customer later.

Scanning documents makes it possible for them to be available to more than one person at a time. It should also reduce the loss of time and money that comes when files are lost or misfiled or checked out and thus not available to others.

## **If records are scanned, is it safe to get rid of the paper originals?**

This topic always draws a lot of interest on the part of records and information managers who share comments and questions by e-mail. There are some who feel that attorneys in particular are loathe to give up the real McCoy, the actual signed document, for a duplication of it as a scanned image.

One RIM professional has devised a schedule for dealing with original paper documents that have been scanned. After scanning, these documents are kept for 30 to 90 days to make sure they have been included in backup, and that there had not been any problems during that time with quality of the scanned images. Within these 90 days, the scanned images have been viewed by those who use them, and if a poorly-scanned page is found, its paper original is retrieved and re-scanned to get a clear image.

Another consideration are the new statutes for electronic discovery added December 1, 2006 to the Federal Rules of Civil Procedure. This means a company involved in federal civil litigation must recognize, declare and produce electronic documents for the trial. Although the new rules provide a standardized framework for e-discovery, they do not address the question of which electronic records must be kept and for how long.

Your storage contractor can be a good source of information on companies that provide scanning, and on the storage needs that may be part of adding scanning to your operation.

## TO BUY OR NOT TO BUY:

### *Identity Theft Spawns New Products and Services To Help Minimize Risk*

Recent headlines about data breaches and losses of personal information have prompted many companies to advertise products or services to help consumers prevent or minimize their risk of identity theft.

The Federal Trade Commission (FTC), the nation's consumer protection agency, says before you pay for an identity theft prevention product or service, make sure you understand exactly what you're paying for. Many people find value and convenience in paying an outside party to help them exercise their rights and protect their information. At the same time, some rights and protections you have under federal or state laws can help you protect your identity and recover from identity theft at no cost. Knowing and understanding your rights can help you determine whether — or which — commercial products or services may be appropriate for you.

#### **Fraud Alerts**

A fraud alert is a signal placed in your credit report or credit file to warn potential creditors that they must use what the law calls "reasonable policies and procedures" to verify your identity before they issue credit in your name. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts.

Under the federal Fair Credit Reporting Act (FCRA), you may be entitled to two kinds of free fraud alerts: initial and extended.

You may ask a consumer reporting company to place an initial fraud alert on your credit report if you suspect you have been, or are about to be, a victim of identity theft. This may be appropriate after your wallet or another source of personal information is lost or stolen. An initial fraud alert is good for 90 days, and can be renewed when appropriate. To place an initial fraud alert, call the toll-free fraud number of any one of the three national consumer reporting companies. The company you call is required to contact the other two; they, in turn, will place an alert on their versions of your report. Expect to receive a confirmation from each of the companies.

Equifax: 1-800-525-6285  
Experian: 1-888-EXPERIAN (397-3742)  
TransUnion: 1-800-680-7289

When you place an initial fraud alert on your credit report, you're entitled to order one free credit report from each of the consumer reporting companies; if you ask, only the last four digits of your Social Security number will appear on your reports.

If you have been a victim of identity theft, you may ask for an extended alert, which stays on your credit report for seven years. To get an extended fraud alert placed

on your report, you will need to contact one of the credit bureaus, and provide an Identity Theft Report, such as a police report or other report to a law enforcement agency, including a report to the FTC. If your credit report has an extended alert, potential creditors must contact you in person, or by phone or some other method you have provided before they can issue credit in your name. When you place an extended alert on your credit report, you're entitled to two free credit reports from each of the consumer reporting companies within 12 months. In addition, the consumer reporting companies must remove your name from marketing lists for pre-screened offers of credit for five years — unless you ask them to put your name back on the list.

#### **Credit Freezes**

A credit freeze allows you to restrict access to your credit report. If you place a freeze on your report, potential creditors and certain other people or businesses can't get access to it unless you lift the freeze temporarily or permanently. For more information about credit freezes, check with your state attorney general's office or visit [www.naag.org](http://www.naag.org).

Limiting access to your credit report makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors will need to view a credit file before opening a new account; if they can't see the file, they may not extend the credit. Still, a credit freeze may not prevent the misuse of your existing accounts or certain other types of identity theft.

A credit freeze is different from a fraud alert in a number of ways. A freeze generally stops all access to your credit report, while a fraud alert permits creditors to get your report as long as they take steps to verify your identity. The availability of a credit freeze depends on state law or a consumer reporting company's policies; fraud alerts are federal rights intended for consumers who believe they may have been, or actually have been, victims of identity theft. And some states charge a fee for placing or removing a freeze, although it is free to place or remove a fraud alert.

Most states have laws that allow consumers to place a credit freeze with consumer reporting companies. In many of these states, any consumer can freeze their credit file; in others, only identity theft victims can freeze their files. The cost of placing a credit freeze and the lead times vary. In many states, credit freezes are free for identity theft victims; other consumers typically are charged about \$10 per credit reporting company. Contact your state attorney general for the particulars of your state's freeze laws. To place a freeze, contact each of the nationwide consumer reporting companies because a credit freeze placed at one company is not referred to the other companies. And be aware that the three major credit reporting companies have begun offering credit freezes directly to consumers — for a fee — regardless of whether their state has a freeze law.

Placing a credit freeze does not affect your credit score, keep you from getting your free annual credit report, or keep you from buying your credit report or score. It

doesn't prevent you from opening a new account yourself, applying for a job, renting an apartment, or buying insurance, either. In these situations, the business usually needs to review your credit report. You can ask the consumer reporting company to lift your credit freeze temporarily, or remove it altogether. But the cost and lead times to lift or remove a freeze vary, so it's wise to check with your state authorities or with a consumer reporting company in advance if possible.

### Free Credit reports

Federal law gives every consumer the right to one free credit report from each nationwide consumer reporting company every 12 months. Staggering these reports — that is, getting a report from a different company every few months — can help you monitor activity on your credit reports. For more information, or to request your free credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com).

### Identity Theft Protection Products and Services for Sale

Identity theft protection companies offer a range of products and services for sale. Some allow you to "lock," "flag," or "freeze" your credit reports. Often, the companies advertising these services simply are offering to place a fraud alert or credit freeze on your report. These services also may renew or update your alerts or freezes automatically, as long as you continue to pay.

Under the law, initial fraud alerts and renewals are available for free if you have reason to believe you have been — or are about to be — a victim of identity theft.

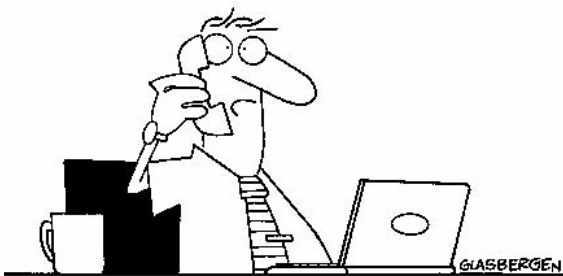
Some companies, including consumer reporting companies, offer subscriptions to credit monitoring services. These services track your credit report, and generally send you an email alert reflecting recent activity, such as an

inquiry or new account. Typically, the more frequent or more detailed the report, the more expensive the service. Some companies offer services to help you rebuild your identity in the event of identity theft. Typically, these services operate by obtaining a limited power of attorney from you, which enables the company to act on your behalf when dealing with consumer reporting companies, creditors, or other information sources.

Many companies may offer additional services, including removing your name from mailing lists or pre-screened offers of credit or insurance, representing your legal interests, "guaranteeing" reimbursement in the event you experience a loss due to identity theft, or helping you track down whether your personal information has been exposed online. Before you agree to pay for any of these services, read the fine print. You can get some of them yourself at no cost: for example, if you decide you don't want to receive pre-screened offers of credit and insurance, you can opt out for five years or permanently by calling toll-free 1-888-5-OPTOUT (1-888-567-8688) or visiting [www.optoutprescreen.com](http://www.optoutprescreen.com).

The FTC has a library of resources to help victims of identity theft report the crime and take steps to recover their identity. Visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit [ftc.gov](http://ftc.gov) or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.



**"You should have received it by now!  
We're not allowed to transmit confidential  
information by telephone, fax, or e-mail,  
so I sent it telepathically."**

### CHECK US OUT!!

If you haven't already, please visit our website for helpful hints and industry news! We are working hard to make our website a valuable resource for you -- our valued customer! [www.thefileroom.com](http://www.thefileroom.com)

### THE BOTTOM LINE: The Benefits of Document Imaging

Thousands of organizations around the world use document imaging every day instead of paper filing systems.

The reasons for this change are simple:

- prevents lost records
- saves storage space
- manages records easily
- finds documents quickly
- makes images centrally available
- eliminates need for file cabinets
- disaster recovery – easy backup

Source: *Forefront Technologies*

*The File Room is a proud member of the following organizations:*

