

### Avoiding the Dumpster Spotlight

It seems that you cannot swing a credit report these days without hitting a local news crew covering a story about records carelessly thrown out in a local dumpster. In fact, a by-product of the sub-prime melt down has been mortgage companies going out of business and leaving loan applications containing personal financial information in the trash. These stories are enjoying media attention because they rightfully concern customers, who have an expectation that their private data are being safeguarded and not tossed in the garbage for anyone to grab.



But, it must also be troubling to business and privacy professionals, too, at least judging from the nearly 65 participants that at the preconference session entitled "Data, Data, Everywhere: Transferring, Selling, Trashing or Destroying Data" at the IAPP's annual Privacy Summit in March. The session covered the problem of disposing of data, both in the ordinary course and in the more complex situation presented by troubled companies and companies in mergers and acquisitions. Here, in a vastly more concise form, are some of the highlights and best practices offered during the session.

#### Legal Requirements

From a legal perspective, there are various federal and state laws and regulations that require records containing sensitive consumer information to be properly cared for and disposed of. More specific laws on the disposal of sensitive data apply, too. To start, many laws require financial institutions and other businesses to provide adequate security, such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), as well as the security-related regulations issued in connection with them. The obligations imposed by these and similar laws do no end at the dumpster's edge. On the contrary, information must be safeguarded at all times.

In addition, there are other laws and regulations that focus on the disposal of sensitive information. For example, the Fair and Accurate Credit Transactions Act, or FACTA, directed the Federal Trade Commission (FTC) to enact rules and regulations governing the disposal of credit reports. In 2004, the FTC promulgated what has become known as the "Disposal Rule." The Disposal Rule requires businesses to take "reasonable measures" to protect against unauthorized access to, or use of, customer information in connection with its disposal, as well as other documents containing information derived from consumer reports.

As covered by the rule, "disposal" is a broad concept, which encompasses abandoning, selling, donating, or transferring, any documents or media containing consumer information. Thus, computer equipment, PDAs, and discs are included. "Reasonable measures" include conducting due diligence on a disposal company, ensuring that papers containing cus-

tom information are burned, pulverized, or shredded, and that electronic files or media containing customer information are properly destroyed or erased. Reasonable measures includes implementing policies and monitoring compliance to ensure the rule is followed.

States have also jumped into this area with different approaches. For example, the state of Texas requires businesses to "destroy or arrange for the destruction of customer records containing sensitive personal information." "Destroy" is further explained to be shredding, erasing, or otherwise modifying a document to make it unreadable. Other states, such as New York, have taken a more precise approach, requiring the destruction of documents that contain specific consumer information, such as Social Security numbers, driver's license numbers, mothers' maiden names, and account numbers. Penalties for non-compliance can be significant, including injunctive relief barring further violations, post-violation auditing requirements, fines and, in some cases, criminal sanctions.

#### Enforcement Efforts

Regulators at all levels are strictly enforcing these laws. In December 2007, the FTC brought an enforcement action against American United Mortgage Company for failure to abide by the disposal rule, resulting in a fine of \$50,000, an obligatory initial and subsequent biennial assessment reports from a third-party auditor, and other compliance monitoring. Likewise, the state of Texas has brought five separate enforcement actions under its own state law, mostly as a result of documents improperly disposed of in dumpsters.

#### Strategies for Compliance

Many garbage disposal companies began offering document destruction services as these disposal rules and regulations began to drive greater business demand. But garbage disposal companies are not in the security business, and they may fail to take measures necessary to meet the Disposal Rule or other legal requirements. Therefore, businesses must be certain to take careful steps to choose the right service provider and comply effectively.

To start, businesses should conduct due diligence before entering an agreement with the disposal company, and make sure to:

- Check References. Ask a potential service provider for references from reputable companies that use its services and make sure to (Continued on Pg. 2)



#### THIS ISSUE:

- **Avoiding the Dumpster Spotlight**
- **Ask The Experts**
- **Gaming Industry Faces Identity Theft**
- **Texas Disposal Settlement**

## Avoiding the Dumpster Spotlight (Continued)

document your contacts with those references.

- **Check Certifications.** The National Association of Information Destruction (NAID) has a Certification Program for Information Destruction Companies to ensure the quality of their disposal programs. Although not a guarantee, a NAID or similar certification is a strong sign that a company takes its responsibilities seriously. Additionally, in October 2008, New York Business Law 899-bbb will become effective. This law requires disposal companies to undergo criminal and other background checks as part of the process to obtain licenses authorizing them to conduct a disposal business.



- **Conduct a Site Check.** Consider visiting the disposal company's site. Is there security to prevent entering into the disposal area? Are logs kept? Are there security cameras? Is the unloading of documents – shredded or yet to be shredded – taking place out in the open, where wind can blow them around the disposal yard? Much can be learned from a site visit during the due-diligence period.
- **Ask for written Policies.** Ask your prospective disposer to provide copies of its internal policies regarding handling of documents to be shredded and their subsequent disposal.
- **Read the Contract.** Be sure to read the proposed service contract and understand what obligations the disposal company agrees to undertake, including the security level of shredding, subsequent recycling or disposing of the shredded material, indemnification and other provisions.
- **Bonding/Insurance.** Disposal companies should have adequate bonding and insurance in the event something goes wrong. Be sure to ask for the declaration page, demonstrating the validity of any insurance.

### Next Steps

Once you have chosen a disposal dealer, there are still a number of internal steps businesses must take to ensure that the process works. Consider the following:

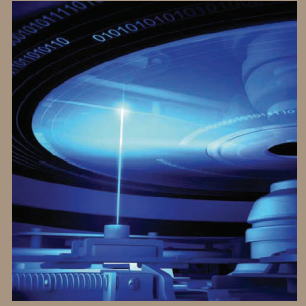
- **Make Containers Convenient.** Make sure to give your employees every reason to use the shredding disposal bin by making it as convenient as possible.

- **Make it Enforceable.** Proper disposal of sensitive documents is a vital part of your business. Make sure that compliance is mandatory and is clearly spelled out in your internal employees policies. Your policies should spell out levels of discipline, up to and including termination, for non-compliance. And of course, be certain to consistently enforce that policy.
- **Establish the Chain of Custody.** Businesses should specify individuals responsible for documents throughout the disposal chain of custody. That is, once documents are placed in the shredding bin, it should be clear whose responsibility it is to make certain that the documents are properly and securely transported to the next step in the process.
- **Determine the Shred Size.** Decide the level of security you wish to achieve in the shredding process. Low security, or simple strip-shredding, may not be suitable for many businesses. Instead, cross-cut, particle-cut, or “granulization” – each providing greater level for disintegration – may be more appropriate. In Europe, there are specific “DIN” standards that apply.
- **Obtain Certificate of Destruction.** Be certain to obtain a certificate of destruction from the disposal company confirming it disposed of the documents. That certificate is not a free pass, but obtaining it is evidence that the business is being diligent about its destruction process. Random/Regular Site Visits. Even after a disposal system is up and running and a business is regularly using a disposal service, it still makes sense to schedule random but regular site visits to your disposer. Once again, look for the same tell-tale signs that the job is being properly conducted – adequate security, backup papers strewn about yard, and the like.

A similar due diligence and policy scheme should be enacted with electronic devices and media as well. Whether you are hiring a service for such disposal, or simply acquiring hardware and software to conduct the disposal internally, be sure to conduct adequate due diligence, establish policies to enforce disposal mechanisms, and audit your disposal efforts to ensure effective compliance.

An effective disposal program is an indispensable part of a business' data privacy efforts; not only will effective compliance ensure that applicable legal requirements are met, but it will prevent the potential damage from having shoddy disposal efforts broadcast on the evening news.

Source: The Privacy Advisor (IAPP), by: Luis Salazar, Elise Berkower, and Greg Dean



### Online Resources

- NAID  
[www.naidonline.org](http://www.naidonline.org)
- ARMA  
[www.arma.org](http://www.arma.org)
- IAPP (International Association of Privacy Professionals)  
[www.privacyassociation.org](http://www.privacyassociation.org)
- EPA  
[www.epa.gov](http://www.epa.gov)
- U.S. Chamber of Commerce  
[www.uschamber.com](http://www.uschamber.com)  
Look for more information on your local Chamber's websites
- Federal Trade Commission  
[www.ftc.gov](http://www.ftc.gov)
- HIPAA – Privacy Rights, Office for Civil Rights  
<http://www.hhs.gov/ocr/hipaa/>
- HIPAA – John Hopkins School of Public Health  
<http://www.jhsph.edu/HIPAA/Links.html>
- Competitors Websites  
Iron Mountain  
[www.ironmountain.com](http://www.ironmountain.com)
- Shred-It  
[www.shredit.com](http://www.shredit.com)
- Recall  
<http://www.recall.com/>

## Ask the Experts: Imaging Means Different Things to Different People

If you would ask a photographer the meaning of the word **imaging** you would probably get a response completely different if you asked the same question to an X-Ray technician.

In the “Business” arena the word **imaging** also has different meanings. I’m just going to give you three different examples associated with **imaging** in the Document Management world.

Imaging at a basic level, within the Document arena, is converting a paper document into an electronic file. The paper is basically nothing more than a carrier mechanism for the data that is written on the paper. Below are three different examples of the different levels of Imaging within the Document Management arena; all of which are services that Cintas can offer.

### **STORAGE & RETREIVAL or ARCHIVE**

If you are housing paper files at your company and they are documents that are stored “After the Business Process” they are primarily kept for referral or legal reasons.

They are rarely added to, or requested, but are needed on occasion. These documents are usually in some sort of File Folder arrangement by Name, Part Number, Customer Number, etc. Cintas can provide a service which allows these documents to be converted into an electronic file. This is usually referred to as “Archival or Storage & Retrieval Imaging Services”.

The process is simple and straight forward. We capture the documents and file them exactly as they are stored in the physical file folders. They can be retrieved exactly how current documents and information is retrieved (i.e. Name, Part Number, Customer Number etc.) Remember that when customers request their converted documents, the electronic file will be the whole file just like they presently receive the file in paper form.

### **APPLICATION SPECIFIC**

More value can be added to the Image if there is application expertise wrapped around it. For example, knowing the process of an invoice that has been received for payment is added value to Cintas’ services. If you understand the “process” associated with a document, then developing a solution is a high value service. Especially if you can replicate that service and resell it again, and again. This is much more than just capturing a paper file and storing it. There are many applications that Cintas’ services fit well within. These include: Accounts Payable, Account Receivable, Human Resource, Payroll, just to name a few.

### **INTEGRATION SERVICES**

One of the more advanced applications that Imaging can perform, and deliver to the customer is high value through the integration of the images into a CORE software that the organization uses. For example, if a company utilize solutions like SAP (Manufacturing), Oracle Financials, Jack Henry (Financial Services) etc, Cintas can offer services where we both manage and integrate the images into the customers’ CORE software. The user of the CORE Software is provided with the image during their processing cycle. This is a very technical-based solution and requires a higher level of imaging experience to develop and sell.

Many CORE software’s of this caliber have existing Document Management “Vaults” already integrated. Cintas also offers capture solutions to migrate the documents directly into their installed vaults.

If you need assistance in any way, please call your “Imaging Expert.”

Written by; Don Byers, CDIA (Certified Document Imaging Architect)



#### **Contact:**

Don Byers – 317-244-8772 (Midwest & National)  
 Randy Thierman – 704-844-0537 (Southeast & National)  
 Bob Hoffman – 904-519-6933 (Florida & National)

## Gaming Industry Faces Identity Theft

Don't think your trash is confidential? Or do you trust your own employees to do their own shredding? The truth is that "70% of information theft is committed by insiders, such as temporary and contract workers, disgruntled employees, and people moving to other companies." (Business Week) This is surprising to many, but don't put your business at risk. The below casino incident is a prime example of employees stealing identities that could be kept safe with the right policies and procedures in place.



### Identity Theft at Seneca Allegany Casino

Officials tell 2 On Your Side, of WGRZ-TV, that a promotions supervisor at Seneca Allegany Casino was activating dormant players cards and loading them up with free slot machine play.

Sandra Whiteeagle was charged with identity theft and conspiracy, among other things, for using the names of 59 casino patrons, and allowing her mother and another person use the cards inside the casino.

As a result, authorities say the suspects won thousands of dollars with the fraudulent players cards. In some cases, the cards were those of deceased patrons.

"They went through this procedure a number of times and probably cost the company \$30,000 to \$40,000. There was no financial loss suffered by any of our patrons. They were simply trying to steal from the company," says Seneca Casino spokesman Phil Pantano.

Seneca gaming officials say this is the first time something like this has happened since the casino opened.

All of the Seneca Casinos have gone through some internal adjustments as a result of the incident to prevent it from happening again in the future.

The three suspects, Sandra White Eagle, Brenda White Eagle and Bradley Stahlman were arraigned in Salamanca last Friday. They could face fines and jail time for the crimes.

Source: WGRZ-TV, Buffalo, New York Posted by: Erika Brason

## Latest Texas Disposal Settlement, Nearly \$1 Million

A national medical company will pay the state of Texas nearly \$1 million after reaching a settlement Wednesday with the state Attorney General's Office over improper discarding of medical records at a Levelland clinic.

Select Physical Therapy Texas Limited Partnership and parent company Select Medical Corp. will pay the state \$990,000 - \$890,000 of which will go to the general revenue fund to be used exclusively for the investigation and prosecution of identity theft cases.

"The overarching message is that in these cases, one of the most important aspects is the defendant will amend procedures to ensure protection of personal information," said Dirk Fillpot, a spokesman for the Attorney General's Office.

Calls and e-mails placed after hours to the Pennsylvania-based medical company were not immediately answered Wednesday evening.

The Attorney General's Office sued the company in January after authorities found more than 4,000 pieces of patient information, including names, addresses, treatment details and bank account and Social Security numbers, in a Dumpster behind the medical company's branch in Levelland. The branch closed in October.

Levelland police discovered the dumped documents after a man and a woman were seen combing through trash in the alley behind the business near 601 S. College Ave., according to a police report.

The company also must implement an amended information security program to protect and safeguard personal information, as a term of the settlement.

Select Texas will be required to designate a corporate employee to serve as a Texas compliance representative to ensure the company complies with the terms of the settlement.

In the future, the company must shred, erase or in some way make sure the personal information contained in records to be discarded is unreadable, according to court documents.

If the company contracts with a third-party provider, the third party also must make records unreadable before they are discarded.

The settlement terms also require the company to train employees within 120 days how to safeguard and dispose of records containing personal information.

If asked, Select Texas must provide the Attorney General's Office a copy of the program and assessments and training materials within 10 business days.

Source: AVALANCHE-JOURNAL By: Logan G. Carver