IDENTITY THEFT: SECURING YOUR COURT DATA

Institute for Court Management
ICM Fellows Program
2015 – 2016 Court Project Phase
May 2016

Lori R. Bienema
Chief Deputy Clerk of Circuit Court
Rock County Circuit Courts
Janesville, Wisconsin

Acknowledgments

Thank you to Wisconsin Supreme Court Former (1996 – 2015) Chief Justice Shirley S. Abrahamson and Wisconsin 5th District Chief Judge James P. Daley for their recommendations that allowed me this opportunity to enhance my analytical skill set and expand my knowledge through the National Center for State Courts Institute of Court Management's certification programs. Thank you to National Center for State Courts Institute of Court Management Dean Daniel Straub, project advisor, for your extraordinary patience and guidance throughout this process. Thank you to Rock County Board of Judges for your unwavering support. Thank you to both former and current Rock County Clerk of Circuit Court for your continued encouragement. Thank you to all Rock County Circuit Court personnel who assisted and participated in the research for this project. Finally, thank you to my family and friends for their patience during this process.

Table of Contents

List of Figures

IDENTITY THEFT: SECURING YOUR COURT DATA

Lori R. Bienema

Abstract

Identity theft and fraud has become the defining crime of the 21st Century. It has been rated the top ranking consumer complaint by the Federal Trade Commission for the past sixteen years. As the third branch of government, the courts are entrusted with sensitive data and must make every reasonable effort to properly protect it. The courts have statutory confidentiality, retention and disposal requirements that must be complied with, however it does not have obligations other businesses must comply with.

There has been a nationwide court implementation converting to electronic record management; with this, the focus of data security has been on electronic security management. Media reports of data breaches, e-mail and telephone scams, employee negligence and/or error, and accidental internet exposure have become commonplace and illustrate the need for a comprehensive data security plan to limit all risks of identity theft and fraud.

Development of an effective comprehensive data security plan begins with assessing the information you maintain and how it moves throughout the court system, including who has access to it and assessing data security vulnerabilities. The most successful security plans comprise physical security, electronic security, employee education and training, and security practices of contractors and service providers.

Without a comprehensive written data security plan for daily operations, court personnel is left to interpret how to secure data and their role and responsibilities in its protection. Educating court personnel in the subject of data security, with an emphasis on personal identifying information (PII), is the key principle in transforming a court environment from “we’ve always done it that way” to a “data security action force”.

While informed court personnel is the best defense against identity theft and fraud, it is only one piece of the puzzle. It is essential for the court to consider the prose user when establishing an effective data security plan, and educating those who the court shares personal identifying information (PII) with, in the subject of data security.

Introduction

According to the Bureau of Justice Statistics, “Identity theft is the attempted or successful misuse of an existing account, such as a debit or credit card account, the misuse of personal information to open a new account or the misuse of personal information for other fraudulent purposes, such as obtaining government benefits or providing false information to police during a crime or traffic stop.” (BSJ). The focus of this court project is to analyze current Wisconsin Circuit (trial) Court practices and processes of safeguarding personally identifiable information (PII) using the Rock County Circuit Courts as a case study and assessing the need for a comprehensive data security plan for the circuit court utilizing key principles as outlined by the Federal Trade Commission (FTC).

As Figure 1 below illustrates in the highlighted area, Circuit Courts in Wisconsin are the trial courts of general jurisdiction. The overall structure is similar to many other states. The trial court level includes courts of limited jurisdiction and courts of general jurisdiction. These are supplemented with a court of intermediate appeals (Court of Appeals) and a court of last resort (Supreme Court). Figure 1 highlights the general jurisdiction courts, known in Wisconsin as Circuit Courts. These courts have exclusive Civil, Domestic Relations and Criminal jurisdiction. The Rock County Circuit Court is the focus of this report.

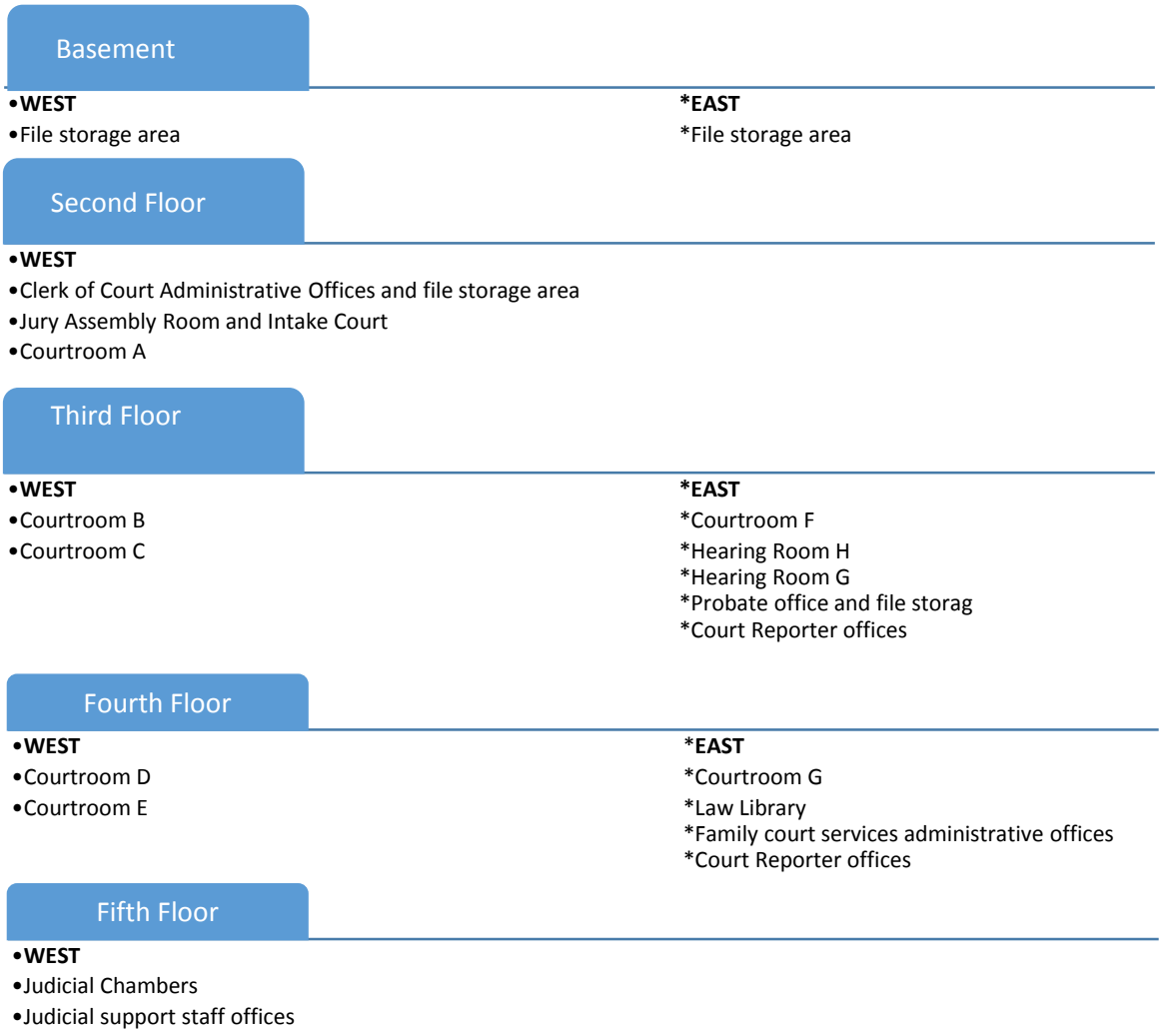
Figure 1. Structure of Wisconsin Courts Highlighting Circuit Courts

`

The Rock County Circuit Court consists of seven circuit courts; housing seven elected circuit court judges, four court commissioners, one elected clerk of circuit court, and fifty two support staff members. The building housing the Circuit Court also houses law enforcement and various county administrative offices. The courts' judicial chambers, courtrooms, administrative office, and support staff workstations are scattered throughout the five story structure. Court record storage areas are located both on-site and off-site. Rock County Circuit Courts are predominately paper based

and are transitioning into electronic file management. The diagram below shows the location of some twenty places within the building (exclusive of the off-site locations) where personal information about court users could at any given time be found.

Figure 2. Potential Locations of Personally Identifiable Information (PII)



The data collected in the project determined how well the Circuit Court is currently protecting personally identifiable information (PII) data by assessing what information courts have, who has access to it, identifying the area at risk, and whether the court is meeting industry data security standards. Four personally identifiable

information (PII) data security processes were evaluated: the daily disposal of paper copies, digital copier/multi-purpose security, network (CCAP) firewalls, and outsourced data.

While entire government websites were located that are dedicated to how private citizens and/or businesses should protect personally identifiable information (PII), similar websites or unified data security plans for the courts were not found. By nature, the courts hold an extraordinary amount of personally identifiable information (PII). How well are the courts handling this data? What are they doing to minimize the possibility of identity theft?

Over the past few years there has been a nationwide push for courts to embrace and implement electronic record management. With this, the focus of data security has been on electronic security management. The available literature suggests that the courts need a unified comprehensive data security plan. This project explores the Wisconsin court practices to determine how the courts are protecting the personally identifiable information (PII) they are entrusted with as well as how they minimize the risks of identity theft exposure.

Two recent events in Philadelphia and Dallas bear repeating in detail as evidence of the potential magnitude and need for comprehensive security planning in the courts.

Philadelphia: Court Documents in the Street

On February 11, 2015 Wendy Saltzman of WPVI Action News wrote the following:

Documents with personal information, such as social security numbers and signatures, were found strewn all over the Grays Ferry section of Philadelphia on Tuesday. We found them after responding to a viewer tip. Action News looked into where the documents came from, and on Wednesday the Philadelphia Common Pleas Court took responsibility. They say they are taking action to make sure this never happens again.

“You don't have to steal identity, when identity is just floating up and down the street. If you wait long enough you can just scoop it up," said resident Basaym Hasan. Hasan told Action News when he walked out his front door he found piles of papers littered across his block. "When I turned them over I noticed personal information was on there such as email addresses, there's social security numbers, there's people's personal information," said Hasan. Many of the documents were marked with the court's seal, leaving residents wondering how such sensitive items got landed at their fingertips.

“You have to shred personal information. I have no idea how it got out here," said resident Darren Erby.

Action News contacted the courts. In a statement, the administrative judge called this an "unfortunate accident" and said they are "investigating how this occurred."

We are now learning the courts do not shred documents on their own because they discard a large number of documents every day. They are instead picked up by the Sanitation Department, which is in charge of destroying those records off-site. The Streets Department today told us "during the tipping process some of the recycling

materials got trapped in a wheel well of one of our recycling trucks and became dislodged as the truck left the plant."

Residents say this isn't the first time they have seen personal records floating up and down their block. "It can be quite embarrassing for the city in a variety of ways to have such information just floating around," said Hasan.

Chief Judge Dougherty in a statement said, "I am not at all comfortable with this system - even prior to this mishap - and have directed our staff to carefully review this procedure and determine what other options might exist that will ensure a more secure handling of sensitive court documents." And the courts also told me there is no industrial shredder that would allow them to shred all those records on site. That is why they have, in the past, depended on this process of having them taken off site for destruction, but they are now reviewing those policies and procedures.

*"*This incident was an unfortunate accident. We are still investigating exactly how it occurred. Regardless, it never should have happened. The long-standing process is that the city's Sanitation Department is responsible for regularly collecting, transporting and destroying old court documents at a city-owned waste facility in Gray's Ferry. I am not at all comfortable with this system - even prior to this mishap - and have directed our staff to carefully review this procedure and determine what other options might exist that will ensure a more secure handling of sensitive court documents."

The Honorable Kevin Dougherty

Administrative Judge Philadelphia Court of Common Pleas - Trial Division

"The Streets Department discovered that during the tipping process some recycling materials got trapped in the wheel well of one of our recycling trucks and became dislodged as the truck left the plant. When we became aware of the problem we immediately dispatched crews to clean the streets in the vicinity of the recycling plant.

We do pick up recycling materials from the Criminal Justice Center. Paper products that are set-out for recycling are handled like any other standard recycling commodity. We process over 125,000 tons of recycling materials per year."

June S. Cantorublic, Relations Specialist II Streets Department

Dallas: Personal Information on the Web

On February 15, 2016 Ginger Allen of the CBS News I-Team wrote:

Your social security number, and your child's, may have been exposed on a government website for more than decade. The CBS I-Team discovered. A major security breach involving tens of thousands of North Texans. And, as shocking as the information being out there is how long I-Team Senior Investigative Reporter Ginger Allen had to pressure Dallas County to fix the problem.

If you file a case in Dallas County Courts, your case documents are public information- accessible by anyone.

But the I-Team discovered some very private information in those files. In a matter of seconds, we found a Dallas' mom's child custody case…and her address, driver's license number, social security number…even, her child's social security

number. The private information was all included in her court documents. It was needed for the court case. But when the I-Team showed the mom all the information we had gathered out of her files by simply logging onto the Dallas County Court online records site, she was stunned. "I'm upset. You have it and who else has it?" said Tiara. She is so concerned about identity theft that she shreds her junk mail. "This is the highest level. This is not some little company mom and pop shop. This is the government that has our information and it's out there for everyone else to get."

Another single mom filed for child support in 2011. The I-Team found her entire file as well as her address, driver's license number, and social security number. "This is how you get credit, a job, my license as a nurse," Collette said stunned. But she was more upset when we showed her that we also had gathered all that information from her file on her two young daughters. Again, we found in it all, in a matter of seconds, on the Dallas County online records site. "I don't even know what to say when I see that," said Collette.

Why Was The Information Out There?

Ike Vanden Eykel heads one of the biggest family practice law firms in Texas. "It's a reasonable conclusion on our part that the government is going to protect that information," said Vanden Eykel studying the cases we printed. "You've got full name, residence, address, social security number, drivers license, home phone…all in one paragraph."

Vanden Eykel says the state pushed electronic filing in the 90's rushing to rid courthouses of paper files. Then, he explained that Dallas County made those files available online for anyone to see. No password required. No protection provided. "When you do something that quickly and that irrationally, you need to expect there are going to be breaches," said Vanden Eykel.

Some attorneys, like Vanden Eykel, who specialize in divorce and family court cases, say they knew they had to protect their client's sensitive information so they removed the private data before filing their cases. But not all attorneys did.

How Many North Texans Are Exposed?

By Dallas County's own admission, tens of thousands of North Texans were exposed according to Dallas County District Clerk Felicia Pitre. The I-Team first contacted the courts about the breach in August 2015. Pitre agreed to an interview about it in October. She told the I-Team her first thought was to shut the online records system down immediately. She is the only person with the authority to do that. She told us, "I wouldn't want my child's information on line. It would cause me grave concern."

But then Pitre later told the I-Team she realized how much attorneys rely on the online files and how taking them away would clog the courts causing an unbearable backlog.

Why CBS 11 Held the Story

As a news organization, CBS 11 decided to the hold the story until she could fix the problem. We did not want to point identity thieves to the sensitive information of tens of thousands of North Texans who could be put at risk. Pitre told us, “It’s an issue. I am concerned.”

But then, weeks turned to months and the information remained out there on line. So, we went back to the District Clerk repeatedly. She said she was working on a fix. By November, we began asking some of the County Commissioners about the issue. We reached out the Court Administrator Daryl Martin. Each official said he or she was very concerned about the information being out there, but no one had the power to shut the system down and take it off line except Felicia Pitre.

I-Team Goes To the Supreme Court

So, the I-Team took the issue to Austin – the Supreme Court of Texas in late November.

“I think we all, every day, need to be concerned that we are putting the public’s information at risk,” responded David Slayton, Court Administrator of the Supreme Court of Texas.

“So you want the public to know that you and the Supreme Court have stepped in and are trying to fix this?” asked I-Team Investigator Ginger Allen.

"Absolutely! The Supreme Court has been looking at this for over a decade," said Slayton explaining that this was a concern of the Justices when e-filing was mandated and counties began making the information available on line. Slayton explained that he had consulted the Justices prior to our visit. Speaking on the Chief Justice's behalf, Slayton told us, "We'll continue (to look into this) until the day we're sure this information is not out there." But Slayton also repeatedly explained that the Supreme Court did not have the power to remove the information from the Dallas County website. Again, he reiterated what so many county officials had told the I-Team— the cases could only be taken off line by the District Clerk. "It's certainly a risk to the public and the individuals whose information is in those records," said Slayton.

Dallas County Commissioners Agree To a Fix

But back in Dallas, in early December, just one day after our visit the Supreme Court, the I-Team learned the Dallas County Court Administrator Daryl Martin deemed this an emergency situation.

District Clerk Felicia Pitre sent the County Commissioners a briefing saying the "sensitive data was inappropriately" included in the Family Court records on line. She asked the commissioners to approve a contract with I-Docket, a company which could remove the sensitive data from the court files. The briefing states the "District Clerk anticipates that the records will be fully available to the public via I-Docket by December 11, 2015.

Nothing Happens – Sensitive Data Remains Accessible To Anyone

Again, as a news organization, CBS 11 decided to hold the story. While we wanted to alert the tens of thousands of North Texans who had sensitive information so easily accessible, we did not want to alert potential identity thieves.

But again, we waited another two months questioning the court, county commissioners, the court administrator, and county judges. We repeatedly reached out to the District Clerk and the Supreme Court by email trying to find out why it was taking so long.

I-Team Emails County Judge

By the end of January, Ginger Allen wrote County Judge Clay Jenkins. While his office returned the call, she never heard directly from him.

However, a week after emailing Jenkins, Court Administrator Daryl Martin told Allen he was holding a meeting to get answers. He explained that I-Docket had successfully removed all of the social security numbers.

Six Months Later – Security Breach Finally Closed

By early February, six months after our investigation began, the Dallas County online records search was removed from the county website. A new link now directs the public to I-Docket, a site which requires your personal information and a fee to access the documents which are now social security number-free. In a paragraph above the link to the new records search, a paragraph states the courts changed the system because of “the growing public concern over identity theft.”

The I-Team repeatedly asked county officials to explain why this process, which put so many North Texans at risk for so long, took so long. No one would comment on camera. Many of them repeatedly told us that Felicia Pitre was an elected official and they did not want to respond.

The I-Team returned to visit Attorney Ike Vanden Eykel after the site was fixed. Attorneys from his office had been part of a committee from the legal community which had been working to fix this site also.

Ginger Allen asked, “Is there any excuse for why this took so long?”

“There is no rational or logical reason for this to have taken six months,” he said repeatedly saying the word ‘shocked’ was an understatement. “Six days would have been way too long.”

This all raises many questions about how long your information may have been out there. One North Texas mother who filed for child support in 2005 told the I-Team she recently had her identity stolen. She wonders if this is why, “They are supposed to protect us and they are giving our information to the thieves,” said Cherlyn.

Why You May Still Need To Contact the Courts

If you have a child custody, paternity, child support, or divorce case that was filed in the Dallas County courts from 2000-2015, you should log on and review your files to make sure that your sensitive data has been removed. The District Clerk told the I-team that those of you who filed cases between 2009 and 2015 should be the most

concerned. If you find personal data in your file, you should contact Dallas County courts immediately to have that information redacted.

******

Both the Philadelphia and Dallas experiences highlight the contemporary need for closer attention to the ways in which courts handle the personal information with which they are entrusted. This project is a step in that direction.

Literature Review

Defining Identity Theft and Fraud

Identity theft and identity fraud are terms used to refer to someone obtaining and using another person's personally identifying information (PII) that involves fraud or deception, typically for financial gain. The Personal Data Privacy and Security Act of 2009 outlines personally identifying information (PII) as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." In 1998 Congressed passed the Identity Theft Assumption and Deterrence Act (Identity Theft Act) into law; since then similar laws were enacted at State levels. Identity theft and fraud causes a financial burden on the justice system as well; costs derive from investigation, prosecution and corrections.

Offenders commonly commit identity theft and fraud by retrieving discarded materials with personally identifying information (PII) that has not been properly disposed of or destroyed; also known as "dumpster diving". Another commonly used method is listening to your conversation to obtain personally identifying information (PII); this is known as "shoulder surfing". Criminals also use internet and telephone scams to commit identity theft and fraud crimes but "dumpster diving" remains the most widespread.

Identity theft and fraud has become the defining crime of the 21st Century. It has been the top ranking consumer complaint to the Federal Trade Commission in recent years. The Bureau of Justice Statistics (BJS) estimates that 17.6 million U.S. citizens experienced identity theft in 2014. The majority of identity theft victims report fraudulent use of an existing account. Economic losses can be measured by direct and indirect losses associated with identity theft and fraud. Indirect losses associated with identity theft are legal and bank fees. The BJS estimated these losses at $24.7 billion in 2012. Victims of identity theft and fraud have also reported emotional costs associated with the crime. Identity theft and fraud reaches across all social and economic groups. Everyone is vulnerable to this crime (See Appendix D).

Special Confidentiality Requirements of Courts

In the State of Wisconsin, the court has a Clerk of Court (custodian of the record) that is governed by local court rules, state statutes and Supreme Court rule. These require the clerk, or his/her designee, to maintain records of all documents filed with the courts, keep a record of all court proceedings, keep records of liens and money judgments, and collect fees, restitution, fines and forfeitures as ordered by the court or statute. The clerk must allow reasonable access to court records in compliance with the Freedom of Information Act (Open Records Law) and maintain confidentiality of records as set forth by statute and court order. Clerks must also comply with statutory retention and disposal of court records; requirements include notice/offering to the State Historical Society. Wisconsin Supreme Court Rule 72.02 states, in part, Records defined as confidential by rule or statute shall be destroyed by burning, shredding or

other means that will obliterate the record. Statutory record retention periods vary by case type and range from five years to one hundred years. (System, 2016)

There are numerous records kept by the court that are statutorily confidential, these records include but are not limited to: juvenile proceedings, john/jane doe proceedings, pre-judgment paternity proceedings, financial disclosure statements, mental proceedings, guardianship proceedings, restraining orders/injunctions involving minors, victim statements, medical/physiological reports and evaluations, sealed and expunged proceedings.

Documents filed and kept by the court contain an abundance of personally identifiable information (PII) of its users, much of which is not statutorily confidential. Traffic, ordinance, and criminal filings include an offender's date of birth, driver license or state identification number, address, height, weight, eye color, hair color, and in some instances fingerprints. Family petitions often include the parties and/or their children's addresses, date of birth, employer, assets, and social security numbers. Civil petitions and complex forfeiture filings can contain tax identification numbers of businesses. Virtually every filing deposited with the court contains personally identifiable information (PII) as outlined by the Personal Data Privacy and Security Act of 2009.

An often overlooked area of records that include personally identifiable information (PII) is the financial/collection area of the courts. When attempting to collect fees, restitution, fines and forfeitures ordered by the court obtaining the debtor's personally identifiable information (PII) is vital to the process. Court collections practices include but are not limited to: wage assignments, tax intercept, deferred payment agreements, and through outside collection agencies.

The Organization Need for Data Security

A breach is defined by the Identity Theft Resource Center (ITRC) as an event in which an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format (See Appendix A).

The Identity Theft Resource Center (ITRC) currently tracks seven categories of data loss methods:

- **Insider Theft**

Example: Department of Children and Families Department of FL, 4/17/2015 - A state employee is behind bars after accessing the personal information of thousands of Floridians. According to the Department of Economic Opportunity, one of their employees managed to access the Florida Department of Children and Families' Florida ACCESS system. He then obtained the names and social security numbers of more than 200,000 people in the DCF system. (ITRC, 2016)

- **Hacking**

Example: Office of Personnel Management Standards, Washington, DC, 6/17/2015 - Regarding the hack of standard personnel records announced last week, two people briefed on the investigation disclosed Friday that as many as 14 million current and former civilian U.S. government employees have had their information exposed to hackers. (ITRC, 2016)

- **Data on the Move**

Example: Sioux Falls VA Health Care System SD, 8/4/2015 - The Department of Veterans Affairs has announced the potential exposure of 1,111 veteran health records after files containing Personally Identifiable Information (PII) and Protected Health Information (PHI) were accidentally tossed in a dumpster. The files were thrown out with regular waste by an employee of the VA Hot Springs Hospital in South Dakota on Friday, May 15, during a move to a different location. The files were mistaken for regular rubbish, and would have remained in the publically-accessible dumpster were it not for a vigilant employee who noticed the dumped files two days later. (ITRC, 2016)

- **Subcontractor/Third Party**

Example: City of Philadelphia - Fire Department EMS Unit PA, 4/2/2015 - The Philadelphia Fire Department learned of a data breach that affects individuals who used its ambulance services. The data breach occurred between June 1, 2012 and October 2, 2012, during which time an employee of Advanced Data Processing, Inc., a subsidiary of Intermedix Holdings Inc., disclosed patient account information to a theft ring involved in a scheme to file fraudulent tax returns with the Internal Revenue Service. Advanced Data Processing, Inc. (conducting business under the name “Intermedix”) handles billing services for ambulance agencies throughout the nation. (ITRC, 2016)

Example: Multi-Function Devices. Fairfax County Virginia. May 2014 - Fairfax County Government discovered that data from multi-function devices was exported by a county contractor, Meridian, from an on-site county server to an Internet-accessible

server owned and maintained externally by Meridian. This unauthorized export occurred in October 2012 by a Meridian technician responsible for supporting these multi-function devices and systems.

Since a 2012 unauthorized data release by the third party vendor, Meridian, managing its multi-function devices used for scanning, faxing and printing documents, Fairfax County Government has contacted, or attempted to contact, individuals impacted by the disclosure of electronic protected health information (ePHI) and personally identifiable information (PII) exposed to the Internet. (ITRC, 2016)

- **Employee error/negligence**

Example: Department of Corrections IL, 8/15/2015 - More than 1,000 Social Security numbers belonging to Illinois Department of Corrections employees were inadvertently released in a response to a Freedom of Information Act request; the documents were sent to a prisoner. (ITRC, 2016)

- **Accidental Web/ Internet Exposure**

Example: Osceola County FL, 10/21/15 - Investigators uncovered an error that allowed personal information of children in Osceola County to go public. Juvenile records are never accessible to the public to protect children. Names of every child charged in and names of children in foster care in Osceola County Florida E-file which provides information on court cases. (ITRC, 2016)

- **Physical Theft**

Example: County of Los Angeles and USC Medical Center CA, 4/30/2015 - Augustus F. Hawkins (Hawkins) Mental Health Center reported that patient records

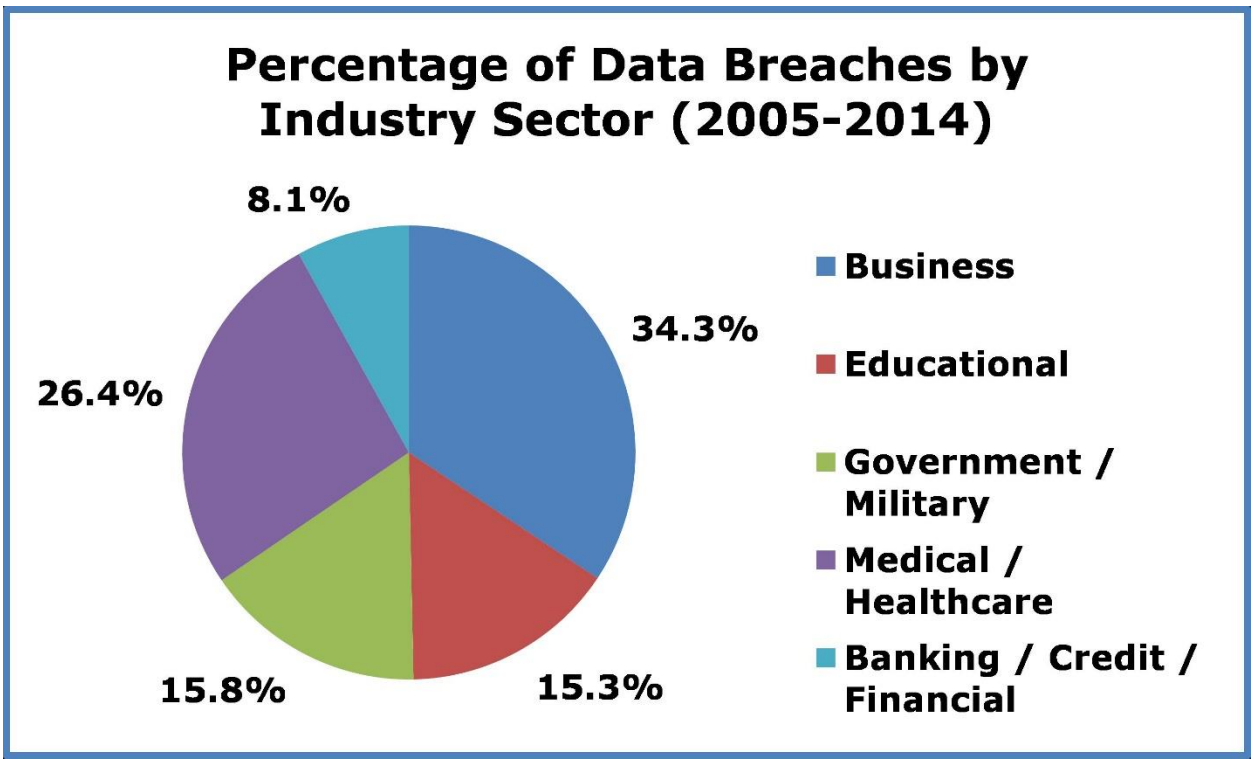
were found in the home of a facility employee, when a search warrant was being served at the residence on April 3, 2015. The search was unrelated to County business, but authorities reportedly found confidential patient information for 900 Hawkins patients in the nurse's home. (ITRC, 2016)

- **Identity Theft Resource Center (IDTRC) Statistical Summaries**

Example: From the 63 known data breaches in 2015 in the Government/Military category, 34,222,763 PII records were exposed; 19% of the 177,866,236 known PII record breaches in 2015.

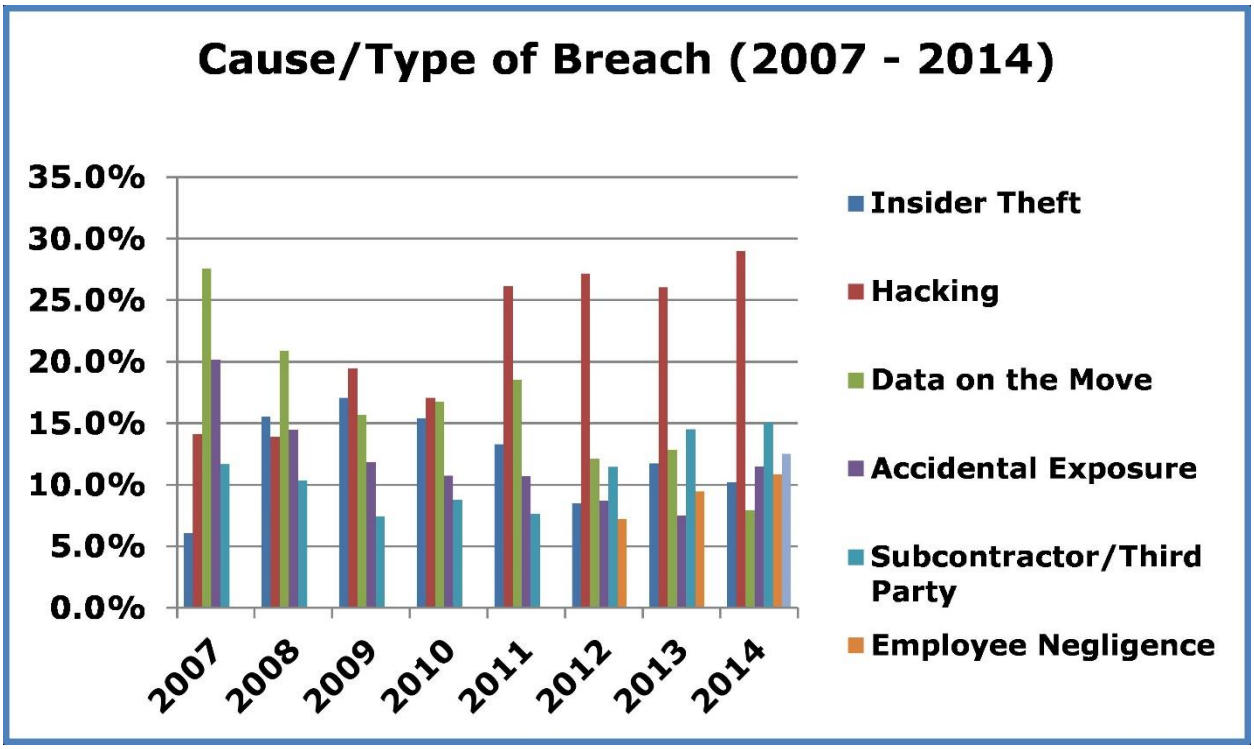
The Identity Theft Resource Center (ITRC) identifies 'Government/Military' as: any city, county, state, national or military entity; or a department within one of these entities. In the event that a medical facility is also a government or military entity, it is listed under Government/Military. Figure 3 below shows the distribution of the more than 5,000 reported breaches and 675 million records exposed since 2005. (ITRC, 2016)

Figure 3. Data Breaches by Industry. (Source: The Identity Theft Resource Center, SAN DIEGO, California – January 12, 2015)



The cause and type of those breaches is shown in Figure 4. Hacking has grown to the overwhelming lead over the eight years listed and employee negligence has risen each year of reporting.

Figure 4. Cause and Type of Breach. (Source: The Identity Theft Resource Center, SAN DIEGO, California – January 12, 2015).



Recommended Best Practices for Information Security

As the third branch of government, the courts, are entrusted with sensitive data and must make every reasonable effort to properly protect it. The courts have statutory confidentiality, retention and disposal requirements that must be complied with, however they do not have obligations other businesses must comply with. Since 2007, many businesses are required to comply with the Federal Trade Commission's Identity Theft Red Flags Regulations and Guidelines promulgated pursuant to section 114 of the Fair and Accurate Credit Transaction Act of 2003 (Red Flags Rule). The Red Flags Rule mandates that financial institutions and other creditors follow a set guidelines in an effort to protect against identity theft and fraud. Although the Red Flags Rule does not apply to the court system, it does offer principles the court system could employ in efforts to protect sensitive information.

At its foundation, the Red Flags Rule is designed to detect, prevent, and mitigate identity theft. It is essential a written data security plan be developed and implemented. Development of an effective data security plan begins with assessing the information you maintain and how it moves throughout your system, including who has access to it and assessing data security vulnerabilities. The most successful security plans comprise physical security, electronic security, employee education and training, and security practices of contractors and service providers.

Physical Security

The majority of data compromises are through paper documents being stolen or improperly disposed of. Vulnerabilities can be drastically reduced through limiting access, employee training, and securing file storage areas.

Maintaining a current inventory of all equipment that holds or collects sensitive data and who has access to it; inventory all computers, digital copiers, PIN pads, court stenograph equipment, smartphones, flash drives laptops and other mobile devices. (Commission, Federal Trade Commission ftc.gov/idtheft, 2015)

Electronic Security

General network security begins with identifying and understanding how your sensitive information is stored electronically. Identify what types of electronic data you receive, share, and maintain through the equipment and how it is accessed/controlled.

The Federal Trade Commission (FTC) recommends to control access to sensitive information by limiting employee access by designating specific user security options; employees should only have access to what is needed to complete their assigned tasks. Employees should be encouraged to use ‘strong’ passwords and change it frequently. Passwords should include mix of letters, numbers, and characters; discourage employees from using their name or other easily deciphered passwords. Use password-activated screen savers to lock employee computers after a period of inactivity. Employees need to be educated on the use and risk of emailing; including the prevention of cyber-attacks and malware by not opening emails from unknown

origins and the importance of managing the sensitive data they send by email to other sources both internally and externally.

The Federal Trade Commission (FTC) recommends the use of wireless and remote access through laptops and other mobile devices should be strictly limited to employees that have a legitimate need and are required to work outside of your customary secured work areas. It is imperative these employees understand the risks and responsibility of being assigned these devices for remote access. Standard protocols for wireless and remote access require the user enable wiping software and storing devices in a secured area; for added protection, your internal Information Technology department should add encryption so the user cannot download any software without prior approval, encrypt transmissions from wireless devices to prevent an intruder from gaining access to your network, and add an "auto-destroy" function in case of theft. Employees must make every effort to secure devices at all times to prevent theft especially while traveling; if a device must be left in a vehicle it should be locked in a trunk, if a device must be taken to an airport it should be included in a carry-on bag and monitored throughout the airport security process.

Digital copiers, fax machines, and stenographer equipment should not be discounted when considering your electronic security plan as these types of equipment contain hard drives which store sensitive data. Often, digital copiers are leased through an outside vendor, stenographer equipment is privately owned by the court reporter, and fax machines are discarded or even auctioned when no longer used or functioning. Regardless of the ownership of the equipment, safeguards to secure sensitive data need to be established. Involvement of your internal Information Technology

department is critical. They can add the necessary data security features, encryption, and overwriting features to the hard drives to ensure security of your sensitive data. Additionally, before you replace the equipment the hard drives should be removed and properly destroyed by your internal Information Technology staff. (Commission, Federal Trade Commission ftc.gov/idtheft, 2015)

Employee Training

A data security plan will only be effective if employees receive proper training. Spend face-to-face time explaining the importance of data security, the role they have in protecting the information, and how to identify potential vulnerabilities and whom they should notify. Informed employees will be your best defense in mitigating risks; keep employees abreast of latest security threats to sensitive data such as national scams and data breaches.

Methods

Three research methods were utilized in assessing the court's data security including document tracking, review of pertinent "standards" sources, and archival data collection.

Tracking Research – The "Dumpster-Diving" Project

As noted previously, the technique known as dumpster diving is a useful unobtrusive method for gaining feedback on an organization's data security without invoking an active response from the members of the organization. An unobtrusive research method uses unusual data sources, i.e., garbage, graffiti, obituaries, worn floor tiles in high traffic areas, and even published statistics. For this project the paper documents in trash and recycle bins were collected to identify those that contained personally identifiable information (PII). That process included the following **on-site** in the courthouse:

- Number of collections: 4
- Collection period: 6 months
- Areas of collection: all court personnel workstations, courtrooms, and shared (by court personnel) areas.
- Collected by: local court administrators

To obtain an accurate account of what sensitive information was in the trash and recycle receptacles and maintain the integrity of the collecting activity no court personnel were made aware of the collection, with the exception of the presiding judge. Should personnel be made aware of the collection process it could potentially alter their

daily disposal habits. However, the first collection was discovered by employees within one day. Many employees voiced distress over the collection of materials they had discarded, but this opened a dialogue about the importance of data security and what was personally identifiable information. The employees were made aware that there would be other collections but not made aware of when they would be conducted.

Additionally, certain **off-site** locations were examined in a similar way.

- Number of collections: continual
- Collection period: 6 months
- Areas of collection: Rock County off-site storage facility and storage areas
- Collected by: local court administrators

Local court administrators are frequently required to retrieve court files from the off-site storage facility. Each time the administrators went to the off-site storage facility during the six month collection period they would retrieve documents that were in the trash and recycle receptacles. During one of these collections an exhibit which had been discarded in a recycle receptacle was retrieved, labeled “SEALED MEDICAL RECORDS”. It contained sensitive information. Likewise, during a collection conducted in a storage area, that housed a copier, a family judgment was found that included the parties’ and their children’s dates of birth, social security numbers, addresses, telephone numbers, and assets. All the information was legible. The (skewed) document had been thrown into a recycle bin after the digital copier had jammed.

Review of Pertinent "Standards" Sources

These specific sources provided valuable information in two areas: best practices and statistical data. Nine organizations were particularly useful in this regard:

- **Federal Trade Commission (FTC)**

The FTC is a bipartisan federal agency with a unique dual mission to protect consumers and promote competition. The FTC is a collegial and consensus-driven agency championing the interests of American consumers. The FTC develops policy and research tools through hearings, workshops, and conferences. The FTC collaborates with law enforcement partners across the country and around the world to advance consumer protection and competition missions. (Commission, ftc.gov, 2016)

For the purposes of this project, the Federal Trade Commission proved to be a significant source offering both statistical data and best practices in reference to identity theft and data security.

- **Identity Theft Resource Center (ITRC)**

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a nationally recognized non-profit organization which provides victim assistance and consumer education through its toll-free call center, website and highly visible social media efforts. It is the mission of the ITRC to provide best-in-class victim assistance at no charge to consumers throughout the United States; educate consumers, corporations, government agencies, and other organizations on best practices for fraud and identity theft detection, reduction and mitigation; and, serve as a relevant national resource on

consumer issues related to cybersecurity, data breaches, social media, fraud, scams, and other issues. (ITRC, 2016)

For purposes of this project, the Identity Theft Resource Center was an invaluable source of both statistical data and best practices in reference to identity theft and data security.

- **General Services Administration (GSA)**

The GSA provides workplaces by constructing, managing, and preserving government buildings and by leasing and managing commercial real estate. GSA's acquisition solutions offer private sector professional services, equipment, supplies, and IT to government organizations and the military. GSA also promotes management best practices and efficient government operations through the development of governmental-wide policies. (Administration, 2015)

For purposes of this project, the GSA's impact was specific to best practices in reference to facilities management and equipment contract and leasing agreements.

- **Council of Better Business Bureaus (CBBB) Better Business Bureau (BBB)**

The BBB is one of the nation's recognized leaders in devolving and administering self-regulation programs for the business community. (Bureau, 2015)

For purposes of this project, the BBB offered up-to-date information on reported scams with its "BBB Scam Tracker". However, it did not contribute statistical data or best practices in reference to identity theft and data security.

- **Bureau of Justice Statistics (BJS)**

The BJS mission is to collect, analyze, publish, and disseminate information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. These data are critical to federal, state, and local policymakers in combating crime and ensuring that justice is both efficient and evenhanded. (Statistics, 2015)

For purposes of this project, the Bureau of Justice Statistics proved to be the most relevant statistical data source relating to identity theft and fraud.

- **United States Department of Justice**

The Department of Justice as an executive department of the government of the United States, the Attorney General has guided the world's largest law office and the central agency for enforcement of federal laws. (Justice, 2016)

For purposes of this project, the US Department of Justice provided statutory information, statistical data, and links to other sources including, but not limited to: the Federal Trade Commission, the Bureau of Justice Statistics, and the Office of Justice Programs.

- **Wisconsin Department of Justice**

The Division of Criminal Investigation (DCI) is charged with a purely criminal investigative mission and function. The Division provides extensive training to local, state and federal officers on current issues in law enforcement. (Justice W. D., 2015)

For purposes of this project, the Wisconsin Department of Justice information was limited regarding identity theft best practices but did offer statistical data and offered AG Opinions regarding questions of law (i.e.; statutory redaction requirements).

- **Wisconsin Court System**

The judicial branch is one of three branches of government. It is responsible for interpreting the laws; the legislative branch makes the laws and the executive branch enforces the laws.

Each of the three levels of court in Wisconsin has a different function, but the entire court system shares a commitment to dispensing justice fairly, impartially, and according to the law. This is a cornerstone of our democracy. (System, 2016)

For purposes of this project, the Wisconsin Court System offered framework for best practices as outlined by Wisconsin Supreme Court Rules (SCR).

- **Wisconsin State Legislature**

Law-making is the principal function of the Legislature, and it does this through legislation. Bills are the form of legislation used to create, amend, and repeal laws. Most of the laws are codified in the Wisconsin statutes, the state's legal code.

For purposes of this project, the Wisconsin State Legislature offered statutory requirements.

Archival Research

Archival documents were obtained through Rock County's Facilities Management, Finance, and General Services. These allowed for analysis of the county's various pertinent agreements to assess the extent to which they have provisions for data security. The following documents were reviewed:

- Vendor Service Contracts:

  Facilities custodial services

  Off-site shredding services

- Lease Agreements:

  Digital multi-purpose copier

Contract and lease agreement language was examined to determine if best practices were fulfilled in accordance with the U.S. General Services Administration and met the needs of the court. Specifically reviewed were the contractor/vendor's required compliance with the laws governing the obligations of businesses to securely dispose of confidential consumer information.

Findings

Finding 1: Wisconsin State statutes and Wisconsin's court operation and Rock County policies pertaining to data security of personally identifiable identification (PII) exist, but are limited in scope.

The Wisconsin State Statutes clearly define the court's requirements in reference to confidentiality, retention, and destruction of records. Wisconsin's Court Operations offers best practices with its Standard of Model Recordkeeping publication; readily available to all Circuit Courts personnel in the State of Wisconsin. Notwithstanding the statutes and best practices publications, there are minimal guidelines for day-to-day data security of personally identifiable identification for the court. In an opinion offered by Court Operations documents filed with the court that contain personally identifiable information (PII), that are not statutory confidential or sealed by the court, should not be redacted of personally identifiable information (PII).

Finding 2: Proposed Wisconsin State Statute §801.19 'Protected information in circuit court records' is currently under review for adoption; relating to electronic security (e-filing).

Proposed Wisconsin Statute §801.19 was created in conjunction with proposed Rule Petition 14-03, currently before the Wisconsin Supreme Court, mandating e-filing for Wisconsin Circuit Courts. The proposed statute defines 'protected information' as a social security number, an employer or tax identification number, a financial account number, a driver license number, and a passport number. In part, the proposed statute states 'the parties to the action are solely responsible for ensuring that protected

information does not appear in any document filed by a party……Protected information that is not properly submitted is accessible to the public.' As cited by Wisconsin's Committee on Confidentiality and Redaction, the proposed statue is comparable to states with redaction rules in place; placing the burden of redaction on the parties and not the clerk of courts.

Finding 3: The Rock County court system does not, at present, have a written local employee data security plan.

Without a written data security plan, personnel is left to interpret how to secure data and their role and responsibilities in its protection. Additionally, the lack of a written data security plan has proven personnel sanctions difficult when records are inadequately managed.

Finding 4: Evaluation of Rock County disposal of paper records vendor contracts reveal a lack of uniformity throughout Rock County; however, industry standards are met. The court's participation in security and facilities management is outlined under Wisconsin Supreme Court Rule (SCR) Chapter 68.

Rock County's court system has three separate contracted vendors providing disposal services. The first vendor provides services of on-site daily disposal removal for the court system and administrative offices located in the courthouse. It is a contracted service provided by Rock County General Service and is governed by the General Services Committee. The second vendor provides services of off-site disposal removal for the court system. It is contracted by Rock County Human Services and is governed by the Human Services Board. The third vendor provides off-site document

shredding services for all Rock County administrative offices including the court system. It is contracted by Rock County Purchasing and is governed by the Finance Committee.

The Rock County shredding vendor service contract agreement complies with electronic data security standards as set forth by the Federal Trade Commission, U.S. General Services Administration, and the Wisconsin Department of Justice; supported by excerpts contained in Bid 2014-17 shown below.

- Off-Site shredding shall consist of pick-up of full, locked containers and replacement with empty containers at the various locations. All containers will be locked/secured at all times except when filling or emptying of containers.
- Rock County and contracted vendor shall agree on a mutual day for drop off of empty bins and pick-up for full bins. Drop off/pick up will not be more than once per week for “as needed” accounts.
- Contractor shall follow all FACTA regulations (laws governing the obligations of businesses to securely dispose of confidential consumer information) that are currently in effect.
- Contractor shall be certified by a recognized trade association (such as NAID) for off-site shredding services.
- Price quote must include all costs related to the shredding process such as furnishing of containers, delivery of empty containers, hauling of full containers, shredding of contents and any other related costs. Quoted price shall be an all-inclusive cost-per-pound.

The three vendor contracts were scrutinized by Rock County's Security and Facilities Committee, while the contract formats varied vastly, they did meet industry standards.

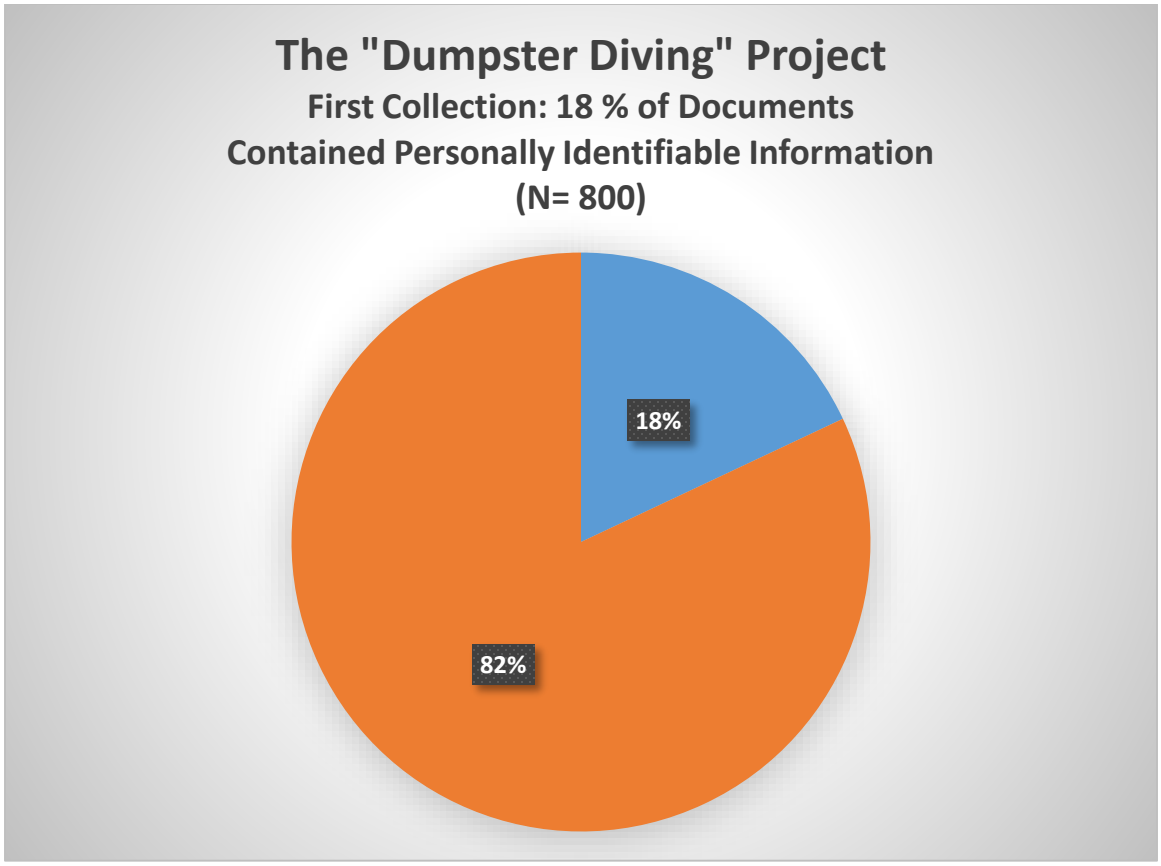
The organizational framework of Rock County's appointed Security and Facilities Committee complies with SCR 68 and is composed of: one circuit judge to serving as chairperson, the chairperson of the county board, the county administrator, the clerk of the circuit court, the county sheriff, the district attorney, one representative of a victim-witness support organization, one circuit court commissioner, and one representative of the facilities/maintenance department.

"SCR Chapter 68 was promulgated by the (Wisconsin) Supreme Court to promote communication among circuit courts, county officials, court planners, architects and contractors concerning court facilities issues…….It is intended to assist counties and courts in making sound decisions about the court facilities that serve the citizens of their Wisconsin communities. This chapter does not create a fixed standard. It is intended to be a statement of general purpose and procedure which establishes a flexible framework for courts' participation in decision-making regarding court facilities while recognizing the wide range of needs and circumstances which exist in counties across the state." (Court, 2011)

Finding 5: The "Dumpster Diving" project results expose inadequate employee education and training of paper document data security.

A staggering 18%, nearly one fifth, of all documents generated from the first sampling contained varying degrees of personally identifiable information (PII).

Figure 5. First Collection Results from the "Dumpster Diving" Project



After the first collection, employees volunteered why they thought this happened. The top response indicated a lack of training and limited understanding what constitutes personally identifiable information (PII). Employees noted that their knowledge was limited to social security numbers. Another notable response was that employees believed documents placed in the recycle bins were shredded by the on-site daily contracted disposal vendors. The number of documents containing personally identifiable information plummeted in the second, third and fourth samplings. The majority of these documents being "screen prints".

Finding 6: The State of Wisconsin's Consolidated Court Automation Program (CCAP) meets electronic data security standards.

The State of Wisconsin's Office of Court Operations fulfills all electronic data security standards (See Appendix B and Appendix C). These areas of standards include, but are not limited to:

- Authorize, assign, and maintain an inventory of equipment users.
- Education and train CCAP uses in electronic data security standards.
- Password management.
- Firewalls, encryption, and security configurations.
- Workstations and servers are kept up-to-date with the latest anti-virus software.
- Alerts and information regarding potential scams are provided to assigned court users and the public; the Better Business Bureau Council reported the 'arrest scam' for skipping jury duty or overdue taxes was the #1 reported scam of 2014 (See Appendix E).

Finding 7: Rock County's digital multi-purpose copier lease agreement safeguards electronic data security.

The Rock County digital copier lease agreement complies with electronic data security standards as set forth by the Federal Trade Commission, U.S. General Services Administration, and the Wisconsin Department of Justice; supported by excerpts contained in Bid 2011-06 shown below.

OPERATING SYSTEMS

The multi-function printers must be compatible with the following:

- Windows, HP-UX, Novell, Linux

HARDWARE

- The scanning option needs to have built-in scan-to-email functionality.
- The scanning option needs to have built-in scan-to-shared-file functionality.
- The scanning feature needs to be TWAIN compliant.
- Preferably, the unit should be able to scan in color even though the printer/copier is specified or configured as black-and-white monochrome.
- Preferably, the scanning feature should support single-pass duplexing.
- The faxing feature needs to allow the user to send a fax from the user's PC.
- The printer needs to have Ethernet network connectivity.

SOFTWARE

- Installer and uninstaller for Windows
- HP PCL 6 and PostScript print drivers for Windows
- Driver management configuration for Windows drivers
- Auto configuration for Windows drivers

IT REQUIREMENTS

- All multi-function printer/copiers must be PCL-6, Postscript Level 3, and direct PDF compatible. The printer/copiers must be LDAP compliant. Additionally, the printer/copiers proposed must be compatible with Rock County's Novell GroupWise e-mail system and must be compatible with HP Webjet Admin for device administration.

SECURITY

- All new equipment purchased shall be equipped with a Hard Drive Data Overwrite Security System which must have the ability to overwrite data nine times.

DISPOSAL OF RETIRED EQUIPMENT

The contracted vendor will assume responsibility of all equipment as it is retired from the fleet. The contracted vendor will remove the hard drive from all retired equipment and give it to Rock County to destroy. Any additional fee for this service must be submitted on attached Proposal Form. The contracted vendor will then be required to remove the retired equipment from Rock County and dispose of it in an environmentally safe manner.

Conclusions and Recommendations

Conclusion 1: Despite statutory confidentiality, retention, and disposal requirements of the court system, the findings reflect an organizational need for local courts to establish written data security plans for day-to-day operations.

Courts have a responsibility to protect those who use its system. Public confidence in the courts could be shaken if entrusted personal identifying information (PII) was perceived as vulnerable. A local written data security plan safeguards day-to-day operations and enhances transparency of the court system.

Recommendation 1: Establish and implement a written data security plan.

Local court judiciary and administration should frequently examine existing local court rules, policies and procedures to assess the effectiveness of the local data security plan. If a local data security plan does not presently exist, one should be created following the Federal Trade Commission's guidelines and standards of data security, coupled with State and Federal statutory requirements. Regardless of whether the court has an existing plan or is creating one, the local data security plan must evolve as potential vulnerabilities are identified. Create an 'environment of security' and encourage court employee's involvement in identifying potential vulnerabilities.

Conclusion 2: E-filing mandates and related statutes do not diminish an organizational need for local courts to establish a comprehensive written data security plan for day-to-day operations.

Statutes and practices relating to mandatory e-filing places the responsibility and compliance of protecting personally identifiable identification (PII) solely in the hands of

the moving party. This may prove problematic as an enormous amount of court users are prose, self-represented litigants. The complexity of the legal system can prove challenging to navigate regardless of the prose litigant's intellect.

Recommendation 2: A local written data security plan must be statutorily compliant and should incorporate mandated e-filing rules and related statutes.

Local court judiciary and administration should examine and incorporate e-filing local and state rules, statutes, and policies and procedures relating to protecting personally identifiable identification (PII) into its local data security plan. The plan should also take into consideration the e-filing system 'prose user'.

Conclusion 3: The "Dumpster Diving" findings illustrates a need for education and training of court personnel in data security.

The "Dumpster Diving" project findings proves alarming, but offers an opportunity for court administration to create an environment of data security for the court. Only through employee application of sound data security practices can court data be adequately secured.

Recommendation 3: Transform your court's work environment from "we've always done it that way" to a "data security action force" through appropriate employee education.

Educating court employees in the subject of data security, with an emphasis on personal identifying information (PII), is the key principle in transforming a court environment. Through education, employees gain an insight as to how their actions or inaction regarding data security can impact the court system.

Court employees should be trained in data security processes as an on-going practice performed by court administration as potential data vulnerabilities and risks evolve.

A written agreement should be created for employees detailing the court's statutory confidentiality, retention, and destruction of records requirements; including the court's day-to-day data security standards (See Appendix F). Management and the bench must be readily available to answer employee questions regarding court requirements and standards to ensure the employee understands the material and is able to successfully carry out their duties. The agreement should include disciplinary measures that will be imposed for failure to comply with requirements and standards. The agreement should be reviewed and signed annually by both administration/management and the employee.

Court administrators need to evaluate each court user's need to access sensitive data information and establish user access security protocols accordingly.

Court administrators should regularly examine employee's compliance with statutory confidentiality, retention, and destruction requirements, best practice policies and procedures, and the local data security plan, to eliminate potential data breaches.

Conclusion 4: Data breaches and identity theft; it could happen to you.

Data breaches and identity theft have become common threats in the 21st Century. A spokesperson for the FBI Cyberdivision articulated the need for electronic data security when he stated, "You're going to be hacked, have a plan". The research

conducted for this report supports the courts need for awareness of personal identifying information (PII) and local data security plans for day-to-day operations.

Recommendation 4: A local court data plan should contain 'user' understanding of electronic data security and a plan in the event of information compromises.

The contents of a local court's data security plan should include 'user' electronic data security measures (i.e., password and email management, and document imaging).

Local courts should ascertain if their state courts have an existing information compromise plan and any statutory requirements. If so, these should be incorporated into their local plan. The type of personal information compromised along with (possible) statutory requirements will determine what actions should be taken. The Federal Trade Commission offers a general guideline if your information is compromised: designate a contact person within your organization for releasing information, notify law enforcement immediately, notify affected businesses/agencies, and notify individuals.

Conclusion 5: Findings confirm a necessity for local court involvement in local county facilities management and vendor service contracts.

The courts operate independently as the third branch of government but are often housed with other branches of government and administrative offices. Vendor services, such as leased equipment and document disposal, are often provided to the courts by contractual vendor services retained and governed by other branches of government and its administration. Court administration should not rely solely on their

county's facilities management services of vendor services and equipment lease agreements. Gone unchecked court data could become vulnerable.

Recommendation 5: The court should be involved in the development and monitoring of facilities management contracts and equipment lease agreements.

Court administration should identify county facilities operations that relate to court data security (i.e.; custodial services), and county general service management of leased equipment relating to court data security (i.e.; digital copier).

Court administration should actively participate in facilities management and lease service vendor bid specifications, vetting, selection, and preparation and monitoring of contractual services processes relating to data security. Court administration should frequently analyze the services provided relating to said contracts and service agreements to verify court standards are being met.

The U.S. General Services Administration (GSA) offers industry standards and best practices relating to facilities management and cooperative agreements. This is a valuable resource for court administrators to employ when participating in county-level facilities and general services management.

References

Administration, G. S. (2015). *gsa.gov*. Retrieved from http://www.gsa.gov/portal/category/100272

Bureau, B. B. (2015). *BBB*. Retrieved from bbb.org: http://www.bbb.org/search/?splashPage=true&type=category&input=idendity+theft&location=&tobid=&filter=webpage&radius=&country=USA%2CCAN&language=en&codeType=YPPA

Commission, F. T. (2015). *Federal Trade Commission ftc.gov/idtheft*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business: https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business

Commission, F. T. (2016). *ftc.gov*. Retrieved from identitytheft.gov: https://www.ftc.gov/sites/all/libraries/infosecurity/

Court, W. S. (2011, June). SCR Chapter 68 COURT SECURITY, FACILITIES, AND STAFFING. *SCR Chapter 68 COURT SECURITY, FACILITIES, AND STAFFING*. Wisconsin.

Dransfield, J. M. (2011-2014). Rock County Bid 2011-06.

Erika Harrell, P. B. (2015, September). *bjs.gov*. Retrieved from Bureau of Justice Statistics: http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408

ITRC. (2016, January). *ITRC Identity Theft Resource Center*. Retrieved from idtheftcenter.org: http://www.idtheftcenter.org/Table/ID-Theft-Blog/ITRC-Surveys-Studies/

Justice, T. U. (2016). *The United States Department of Justice*. Retrieved from justice.gov: https://www.justice.gov/

Justice, W. D. (2015). *Wisconsin Department of Justice*. Retrieved from https://www.doj.state.wi.us/: https://www.doj.state.wi.us/

Statistics, B. o. (2015). *BJS Bureau of Justice Statistics*. Retrieved from www.bjs.gov: http://www.bjs.gov

System, W. C. (2016). *wicourts.gov*. Retrieved from wicourts.gov: http://www.wicourts.gov

Appendix A. Government/Military Breaches 2015 Identity Theft Resource Center (ITRC)

Government/Military: Any city, county, state, national or military entity; or a department within one of these entities. In the event that a medical facility is also a government or military entity, it will be listed under Government/Military. Entities such as Veteran Association Medical Centers (VAMC) will be included in this sector.

- From the 63 known data breaches in 2015 from the Government/Military category, 34,222,763 PII records were exposed; 19% of the 177,866,236 known PII record breaches in 2015.

Department of Health NM, 12/15/2015: A New Mexico Department of Health data breach report indicates 561 patients have had their Protected Health Information (PHI) exposed as a result of the theft of an unencrypted laptop computer from an employee's vehicle. An investigation was conducted to determine what data were stored on the laptop. Some of the information was password protected, although patient first and last names, dates of birth, medications, facility unit, and in some cases, medical diagnoses, were also stored on the laptop and could potentially be accessed by the thief.

Jefferson County CO, 11/24/2015: As public anxiety persists over regular reports of major data breaches, Social Security numbers of up to thousands of current and former Jefferson County residents can be found online in electronic county records, increasing locals' vulnerability to a costly and stressful ordeal.

Department of Human Services Agency MD, 8/18/2015: We are writing to notify you that a letter containing some of your personal information was mistakenly sent to the wrong address. The letter meant for you was inadvertently stuck to another letter and mailed to the wrong individual. When the mistake was discovered, the letter was returned to us immediately. The letter included your name and home address, as well as your case number.

Georgia Secretary of State GA, 11/18/2015: Two Georgia women have filed a class action lawsuit alleging a massive data breach by Secretary of State Brian Kemp involving the Social Security numbers and other private information of more than six million voters statewide. The suit, filed Tuesday in Fulton County Superior Court, alleges Kemp's office released the information including personal identifying information to the media, political parties and other paying subscribers who legally buy voter information from the state.

Maryland Department of Information Technology MD, 11/4/2015: Maryland's Department of Information Technology is admitting to exposing the "Personally Identifiable Information" of hundreds of people and companies that do business with the state by accidentally publishing a list of them on a public website. Data exposed included Social Security and Tax ID numbers.

Department of Motor Vehicles CA, 10/9/2015: On September 28, 2015, a DMV employee was sending a file containing your personal information to the Santa Clara Transportation Agency as part of the agency's Employer Pull Notice (EPN) program. The EPN program provides agencies with a means of promoting driver safety through the ongoing review of driver records. However the employee also sent the file to another government entity by mistake.

Wisconsin Department of Veterans Affairs WI, 10/30/2015: The Social Security numbers of Wisconsin veterans are being sent via email without encryption despite numerous federal laws and U.S. Department of Veterans Affairs regulations requiring personally identifiable information be password-protected. It partly explains how a random Wisconsin veteran received an unsolicited email on April 1 with the Social Security numbers and disability claim information of hundreds of Wisconsin veterans. Since the Vietnam War, veterans' file numbers or disability claim numbers have been their Social Security numbers.

Osceola County FL, 10/21/2015: 9 Investigates uncovered an error that allowed personal information of children in Osceola County to go public. Juvenile records are never accessible to the public to protect children. That's why a sign in front of the clerk's office says, "Juvenile cases are confidential." Reyes found names for every child charged in and names of children in foster care in Osceola County Florida E-file which provides information on court cases.

Department of Health's Children's Medical Services FL, 10/23/2015: About 150 clients of the Florida Department of Health's Children's Medical Services program in Miami-Dade may have had their personal information compromised after vendors were faxed a clinic roster containing names, birth dates and membership numbers, agency officials reported Friday.

Salt Lake County UT, 10/9/2015: On September 9, 2015, Salt Lake County learned of a possible security incident involving Workers' Compensation or other damage claims submitted to the County. On June 18, 2015, a software services company hired by the County improperly set one or more security settings during a scheduled upgrade. While the investigation is ongoing, it appears that the improper settings may have allowed information submitted to the County in connection with Worker's Compensation or other damages claims to be temporarily accessible on the Internet. This information may have included the name, address, limited medical information associated with a claim, and in some cases Social Security numbers of claimants.

Department of Health and Human Services NC, 10/17/2015: The state Department of Health and Human Services says a breach of security protocol may have compromised the confidential health information of 1,615 Medicaid patients. According to the agency, a DHHS employee "inadvertently sent an email to the Granville County Health Department without first encrypting it." The email included a spreadsheet containing protected health information for Medicaid recipients, which the agency says "included the individual's first and last name, Medicaid identification number (MID), provider name and provider ID number, and other information related to Medicaid services."

Ferndale Housing Commission MI, 10/4/2015: Illegal dumping in Detroit is not uncommon - but one case in Brightmoor is especially alarming. It was bad enough to have to look at the mess, but what Graham Emerson found recently was enough to send the grizzled Detroiter over the top. A moderate pile of junk included personal documents from the Social Security Administration and the Ferndale Housing Commission.

Pentagon Food Court VA, 9/9/2015: "Within the past week, the Pentagon Force Protection Agency has received numerous reports of fraudulent use of credit cards belonging to Pentagon personnel. These individuals had fraudulent charges to their account soon after they had legitimate transactions at the Pentagon," according to a copy of the notice to employees obtained by the Washington Examiner. Hackers infiltrated the Pentagon food court's computer system, compromising the bank data of an unknown number of employees

Department of Corrections IL, 8/15/2015: More than 1,000 Social Security numbers belonging to Illinois Department of Corrections employees were inadvertently released in a response to a Freedom of Information Act request.

VA Black Hills Health Care System SD, 8/1/2015: Human error strikes the VA system again. Seth Tupper reports that someone at the VA Black Hills Health Care System mistakenly dumped a box containing 1,100 veterans' files into a dumpster on May 15. The error occurred during an office move (a problem we've seen before in other cases)

Department of Child Safety AZ, 8/4/2015: A batch of documents from the Department of Child Safety was found in a Kingman dumpster. They contained personal information including names and social security numbers. The documents reportedly contained detailed descriptions of investigations.

Sioux Falls VA Health Care System SD, 8/4/2015: The Department of Veterans Affairs has announced the potential exposure of 1,111 veteran health records after files containing Personally Identifiable Information (PII) and Protected Health Information (PHI) were accidentally tossed in a dumpster. The files were thrown out with regular waste by an employee of the VA Hot Springs Hospital in South Dakota on Friday, May 15, during a move to a different location. The files were mistaken for regular rubbish, and would have remained in the publically-accessible dumpster were it not for a vigilant employee who noticed the dumped files two days later

Indiana Department of Revenue IN, 7/18/2015: Indiana Department of Revenue, 1,262, cause unavailable (electronic).

Department of Corrections and Rehabilitation CA, 5/7/2015: On May 7, 2015, we discovered that the Gate Clearance document you submitted to Mule Creek State Prison was electronically scanned and stored to a computer folder where employees outside of Plant Operations may have been able to read it. The document contained your name, Driver License number and Social Security number. Immediately upon discovery, access to the folder was secured to only allow access to the Plant Operations employees.

Army National Guard VA, 7/11/2015: The U.S. Army National Guard experienced their own personnel data breach, they announced Friday. The data breach includes current and former soldiers' names, full Social Security numbers, dates of birth and home addresses.

Department of Aging and Disability Services TX, 6/11/2015: On June 11, the Texas Department of Aging and Disability Services announced that the protected health information of approximately 6,600 Medicaid recipients may have been released unintentionally. The agency stated that a web application intended for internal use only was accessible on the Internet. The application contained patients' names, residences, addresses, birth dates, Social Security numbers, medical diagnoses and treatment information.

Office of Personnel Management Standards DC, 6/17/2015: Regarding the hack of standard personnel records announced last week, two people briefed on the investigation disclosed Friday that as many as 14 million current and former civilian U.S. government employees have had their information exposed to hackers, a far higher figure than the 4 million the Obama administration initially disclosed. (includes 2 million relatives and other associates)

Office of Personnel Management DC, 6/4/2015: Hackers broke into the U.S. government personnel office and stole identifying information of at least 4 million federal workers. The Department of Homeland Security said in a statement Thursday that at the beginning of May, data from the Office of Personnel Management and the Interior Department was compromised. (Current and former government employees)

Town of Brunswick ME, 5/15/2015: On April 28, 2015, the Brunswick Police Department discovered that an unredacted copy of its March 2, 2015 police log had been inadvertently sent to four media outlets, one of which published the information online. We immediately took steps to notify the media outlet of this incident and confirm complete removal of this information from its website

Department of State FL, 5/26/2015: For the second time in two months, Gov. Rick Scott’s administration has acknowledged it a confidential personal data of private citizens, prompting the state to offer free credit monitoring services to protect people from being victims of identity theft

Internal Revenue Service (IRS) DC, 5/27/2015: The IRS announced today that criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through IRS’ “Get Transcript” application. This data included Social Security information, date of birth and street address

County of Los Angeles and USC Medical Center / Augustus F. CA, 4/30/2015: Augustus F. Hawkins (Hawkins) Mental Health Center reported that patient records were found in the home of a facility employee, when a search warrant was being served at the residence on April 3, 2015. The search was unrelated to County business, but authorities reportedly found confidential patient information for 900 Hawkins patients in the nurse's home. (www.dhs.lacounty.gov)

VA Long Beach Healthcare System CA, 4/20/2015: Documents containing the personal information of veterans seeking treatment at the Veterans Affairs Long Beach Hospital may have been improperly disposed, Veterans Affairs officials said. Army veteran and hospital patient Paulnhu Nguyen said he found a large stack of patient records containing personal information, such as social security numbers, date of births and full names, in a dumpster by the hospital after his appointment on Thursday

Department of Children and Families / Department of FL, 4/17/2015: A state employee is behind bars after accessing the personal information of thousands of Floridians. According to the Department of Economic Opportunity, one of their employees managed to access the Florida Department of Children and Families' Florida ACCESS system. He then obtained the names and social security numbers of more than 200,000 people in the DCF system.

Denton County Health Department TX, 4/10/2015: On February 13, 2015, a Denton County Health Department employee temporarily left a USB drive at a local printing store in order to print a personal document from the device. Unfortunately, that USB drive included 874 unsecured data files of tuberculosis (TB) clinic patients belonging to the Denton County Health Department, including patient names, dates of birth, addresses, TB test results and other protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA). The data files did not include any financial information or any social security numbers

City of Philadelphia - Fire Department EMS Unit PA, 4/2/2015: The Philadelphia Fire Department (the "Fire Department") learned of a data breach that affects individuals who used its ambulance services between February 1, 2012 and September 4, 2012. The data breach occurred between June 1, 2012 and October 2, 2012, during which

time an employee of Advanced Data Processing, Inc., a subsidiary of Intermedix Holdings Inc., disclosed patient account information to a theft ring involved in a scheme to file fraudulent tax returns with the Internal Revenue Service. Advanced Data Processing, Inc. (conducting business under the name “Intermedix”) handles billing services for ambulance agencies throughout the nation, including Emergency Medical Services (“EMS”), the unit of the Fire Department that provides ambulance services in Philadelphia

Department of Business Oversight CA, 4/7/2015: The California Public Records Act (PRA) requires the Department of Business Oversight (DBO) to provide the public copies of the nonconfidential portions of our electronic licensing records upon request. To process these requests, DBO utilizes the records contained in the Financial Industry Regulatory Authority’s (FINRA) Central Registration Depository (CRD). Fields clearly designated as containing personal identifying information within the FINRA CRD are then redacted by DBO prior to its release. However, despite our efforts, DBO recently learned that, pursuant to one or more PRA requests, the personal identifying information of a number of registered investment advisers and broker-dealers was inadvertently disclosed to persons not authorized to receive such information.

Department of Labor VT, 3/20/2015: The Vermont Department of Labor has determined a now-former employee improperly obtained "personally identifiable information" including names and Social Security numbers from its unemployment insurance program database. A criminal investigation into possible identity theft is underway, officials said. At least 80 people are affected by the breach. Also at least seven businesses have been compromised, officials said.

GA Department of Community Health GA, 3/2/2015: Georgia Department of Community Health GA Health Plan 355127 03/02/2015 Hacking/IT Incident Network Server

County of Haywood NC, 2/9/2015: Haywood County NC Healthcare Provider 955 02/09/2015 Loss Paper/Films

VA Corporate Data Center Operations / Austin TX, 1/7/2015: VA Corporate Data Center Operations/Austin Information Technology Center TX Healthcare Provider 7029 01/07/2015 Hacking/IT Incident Network Server

Philadelphia Common Pleas Court PA, 2/16/2015: Documents with personal information, such as social security numbers and signatures, were found strewn all over the Grays Ferry section of Philadelphia on Tuesday.

We are now learning the courts do not shred documents on their own because they discard a large number of documents every day. They are instead picked up by the Sanitation Department, which is in charge of destroying those records off-site.

Lubbock Housing Authority TX, 1/20/2015: Representatives of the Lubbock Housing Authority are asking anyone who filled out a Section 8 application to call their office, as personal information may have been breached. Mike Chapman, executive director, said because the program is so popular — and officials want the selection process to be fair — employees compile all the applicants into one spreadsheet and then do a random sort to place them in order on the waiting list. He compared the system to a lottery. He said the file mistakenly put on the website contained the applicants' whole Social Security numbers and estimated income, along with their names and addresses

St. Louis County's Department of Health MO, 1/15/2015: St. Louis County has learned that some personal information belonging to inmates was handled inappropriately at the St. Louis County's Buzz Westfall Justice Center. Specifically, on November 18, 2014, it was discovered that a health department employee had e-mailed a document containing the names and social security numbers of inmates incarcerated from 2008 to 2014 to a personal e-mail account belonging to that same employee. Although no one other than that county employee is known to have had access to the information in that document, the action still constitutes a breach of federal law – specifically, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). [County Department of Health]

Appendix B. Wisconsin court data site to implement "CAPTCHA" protection

Madison, Wisconsin - September 25, 2015

On Sept. 28, the Wisconsin court system will implement a CAPTCHA feature on its Wisconsin Circuit Court Access (WCCA) website to help prevent automated attempts to extract circuit court data from the website.

CAPTCHA is a widely used challenge-response program that enables a website to determine whether a visitor is a human being or an automated "screen scraping" program. The WCCA website receives between three and five million page views per day, and the number of suspected screen scrapers is increasing.

WCCA users will be required to respond to a question the first time they perform a search and will be re-verified after every 10 searches. This feature will be implemented for all WCCA search screens, including: Search (simple, advanced, and judgment); Calendars; Pay fees online; and Reports.

The WCCA website provides convenient access to online public circuit court records. However, a high volume of screen scraping slows down service for other public users and may result in deceitful practices, such as scams promising to remove court records from a website in exchange for payment. Any business or website offering to remove court case information for payment is not connected to WCCA or to any circuit court. Wisconsin circuit courts do not accept payment to remove court case information from the website.

Public case information is posted on the WCCA website under the terms of a Policy on Disclosure of Public Information over the Internet and a record retention policy set by Supreme Court Rule. More information about WCCA can be found in a Frequently Asked Questions section of the website.

Many CAPTCHA programs ask website visitors to retype the letters, numbers or symbols contained in a distorted image. The WCCA CAPTCHA program will work similarly but will ask visitors to identify certain types of images or objects, such as food.

For companies or individuals who wish to download bulk data, Consolidated Court Automation Programs (CCAP) provides a subscription-based service using an automated program.

Appendix C. Policy on Disclosure of Public Information over the Internet

1. Definitions:
    a. The definitions contained in the Open Records Law, Wis. Stats. §§ 19.21-.39, shall apply to this policy.
    b. *Consolidated Court Automation Programs (CCAP)*. The case management system created by the Wisconsin Director of State Courts consisting of a database of case information from Wisconsin circuit courts. References in this policy to actions to be taken by CCAP refer to the CCAP Steering Committee or the Director of State Courts.
    c. *Circuit court*. All offices and branches of a circuit court, including but not limited to judges, the clerk of circuit court, the clerk's deputy, or deputies; probate court; juvenile court; or other specialized court or court office that uses CCAP as a case management system.
    d. *Open records*. Those records that are by law accessible to an individual making a records request in the circuit court.
    e. *Confidential records*. Those records that are not by law accessible to an individual making a records request in the circuit court.
    f. *Wisconsin Circuit Court Access (WCCA)*. A public-access Internet website containing open record information compiled by CCAP. References in this policy to actions to be taken by WCCA refer to the WCCA Oversight Committee.
2. Information on WCCA available to the general public:
    a. WCCA shall contain information from only those portions of the case files generated by the Consolidated Court Automation Programs (CCAP) that are open records and otherwise accessible by law to an individual.
    b. WCCA shall not contain information from closed records that would not otherwise be accessible by law to an individual because of specific statutory exceptions, such as juvenile court records, guardianship proceedings, and other such case types or records.
    c. CCAP shall not be required to make available on WCCA all information in a case file that may be public record, nor is CCAP required to generate new records or create new programs for extracting or compiling information contained on WCCA.
    d. The Open Records Law does not allow record custodians to demand either the identity of a requester or the use to which a requester intends to put the information gathered [Wis. Stats. § 19.35(1)(i),]. Accordingly, WCCA shall not require identification or an intended purpose before allowing public access to the WCCA website.
    e. WCCA shall not charge for accessing information through the website. However, WCCA may impose a service charge or assess user fees for requests for bulk distribution or for data in a specialized format.
    f. WCCA may limit the number of records searched on any single request.
    g. WCCA contains information as it exists at a specific point in time in the CCAP database. Because information in the CCAP database changes constantly, WCCA is not responsible for subsequent entries that update,

modify, correct or delete data. WCCA is not responsible for notifying prior requesters of updates, modifications, corrections or deletions. All users have the responsibility to determine whether information obtained previously from WCCA is still accurate, current and complete.

h. WCCA shall not contain:
    a. the record of any criminal conviction expunged by the circuit court (Note: When a court orders expunction of a record, the underlying CCAP database is modified to remove the record. When database updates are transferred to WCCA, the previous record will no longer appear. WCCA makes no reference to records that have been expunged (or otherwise altered). Requests for such records report only that no record has been found, in the same manner that WCCA would otherwise report "null" searches. WCCA is not responsible for the fact that requests made before the expunction will show the conviction, while requests made after the expunction will not show the conviction.)
    b. the "day" from the date of birth field for non-criminal cases
    c. the driver's license number in traffic cases
    d. "additional text" fields for data entered before July 1, 2001, in all cases.
i. WCCA contains only information from the CCAP database from those counties using all or part of the CCAP system. Because extraneous actions are not normally reflected in the CCAP database or the circuit court files, WCCA does not include information on them. Examples of extraneous actions are gubernatorial pardons, appellate decisions, and administrative agency determinations.

3. Correcting information on WCCA:
    a. Neither CCAP nor WCCA creates the data on WCCA. Circuit court employees in counties using CCAP create the data. Neither CCAP nor WCCA is responsible for any errors or omissions in the data found on WCCA.
    b. An individual who believes that information on WCCA is inaccurate may contact the office of the clerk of circuit court in the county in which the original case file is located to request correction.
    c. The clerk of circuit court in the county in which the original case file is located shall review requests for corrections and make any appropriate corrections so that records on WCCA reflect the original case records.
    d. Corrections shall be entered on CCAP and will be made available on WCCA in the same manner in which information is otherwise transmitted to WCCA.

4. Privacy for victims, witnesses and jurors:
    a. The data fields that contain the names of victims, witnesses and jurors are not available on WCCA.
    b. Various documents completed by court personnel using CCAP occasionally require the insertion of names of victims, witnesses or jurors. Examples include:
        1. court minutes that provide the names of witnesses called to testify or jurors who have been considered for jury duty;
        2. judgments of conviction that may provide "no-contact" provisions concerning victims;
        3. restitution orders that may contain the name of a victim;
        4. restraining orders/injunctions that may provide victim identities.

        These data elements are normally inserted into "additional text" fields by circuit court personnel based on the individual county's policies and procedures on the amount, detail, or type of data inserted. CCAP and WCCA recommend that court personnel entering information concerning crime victims into court documents use initials and dates of birth rather than full names whenever doing so would not defeat the purpose of the court document.

    c. Because the "additional text" fields contain information critical to the understanding of many of the court record entries, denying access to those fields because of the occasional inclusion of the name of a victim, witness or juror would be contrary to the public interest in providing meaningful access to open court records.

5. Public access to electronically filed documents, scanned documents or imaged documents contained in circuit court files:
    a. WCCA shall evaluate whether to provide access to documents that have been filed electronically, scanned or otherwise imaged by the circuit court so long as those documents would otherwise be fully accessible under this policy.
    b. The electronic filing, scanning or imaging of some documents in a court file does not require that all other documents in that file be scanned or imaged.
    c. The electronic filing, scanning or imaging of some documents in files in a case type does not require that all documents in all other files in the same case type must be scanned or imaged.

6. Non-public access to closed records available on CCAP:
    a. CCAP may maintain a non-public website that contains information that would otherwise be a closed record.
    b. CCAP may authorize an appropriate law enforcement agency, prosecutor's office or other individual or agency electronic access to those closed records to which they would otherwise be entitled to access.
    c. CCAP may require an appropriate security screening mechanism that limits the accessibility to closed records to those who are lawfully entitled to such access.
    d. Authorization to access closed records for legitimate purposes is not authorization for redisclosure beyond that which is lawfully allowed. The individual or agency to which disclosure has been allowed is solely responsible to ensure that no further unauthorized redisclosure of closed records occurs.

19.31 Declaration of policy. In recognition of the fact that a representative government is dependent upon an informed electorate, it is declared to be the public policy of this state that all persons are entitled to the greatest possible information regarding the affairs of government and the official acts of those officers and employees who represent them. Further, providing persons with such information is declared to be an essential function of a representative government and an integral part of the routine duties of officers and employees whose responsibility it is to provide such information. To that end, ss. 19.32 to 19.37 shall be construed in every instance with a presumption of complete public access, consistent with the conduct of governmental business. The denial of public access generally is contrary to the public interest, and only in an exceptional case may access be denied.

Appendix D. Bureau of Justice Statistics Press Release

ADVANCE FOR RELEASE AT 10:00 A.M. EDT	**Bureau of Justice Statistics**
SUNDAY, SEPTEMBER 27, 2015	**Contact: Kara McCarthy (202) 307-1241**
HTTP://WWW.BJS.GOV/	**After hours: (202) 598-9320**

17.6 MILLION U.S. RESIDENTS EXPERIENCED IDENTITY THEFT IN 2014

WASHINGTON – An estimated 17.6 million persons, or about 7 percent of U.S. residents age 16 or older, were victims of at least one incident of identity theft in 2014, the Bureau of Justice Statistics (BJS) announced today. These statistics were similar to those in 2012.

Identity theft is the attempted or successful misuse of an existing account, such as a debit or credit card account, the misuse of personal information to open a new account or the misuse of personal information for other fraudulent purposes, such as obtaining government benefits or providing false information to police during a crime or traffic stop.

In 2014, the most common type of identity theft was the unauthorized misuse or attempted misuse of an existing account—experienced by 16.4 million persons. Victims may have experienced multiple types of identity theft. An estimated 8.6 million victims experienced the fraudulent use of a credit card, 8.1 million experienced the unauthorized or attempted use of existing bank accounts (checking, savings or other)

and 1.5 million victims experienced other types of existing account theft, such as misuse or attempted misuse of an existing telephone, online or insurance account.

Most identity theft victims discovered the incident when a financial institution contacted them about suspicious activity (45 percent) or when they noticed fraudulent charges on an account (18 percent). The majority of identity theft victims did not know how the offender obtained their information, and 9 in 10 identity theft victims did not know anything about the offender.

Two-thirds of identity theft victims reported a direct financial loss. Victims whose personal information was misused or who had a new account opened in their name experienced greater out-of-pocket financial losses than those who had an existing credit card or bank account compromised. About 14 percent of identity theft victims experienced an out-of-pocket loss of $1 or more. Of those, about half suffered losses of $99 or less and 14 percent lost $1,000 or more.

The majority of identity theft victims (52 percent) were able to resolve any problems associated with the incident in a day or less, while about 9 percent spent more than a month. Victims who spent more time resolving the associated problems were more likely to experience problems with work and personal relationships and severe emotional distress than victims who resolved the problems relatively quickly. Among identity theft victims who spent six months or more resolving financial and credit problems due to the theft, 29 percent experienced severe emotional distress, while 4 percent who spent a day or less experienced such distress.

In 2014, fewer than one in 10 identity theft victims reported the incident to police. The majority (87 percent) of identity theft victims contacted a credit card company or bank to report misuse or attempted misuse of an account or personal information, while 8 percent contacted a credit bureau.

Other findings include—

- In 2014, 85 percent of people took actions to prevent identity theft, such as checking credit reports, shredding documents with personal information and changing passwords on financial accounts.
- The number of identity theft victims age 65 or older increased to 2.6 million in 2014— up from 2.1 million in 2012.
- More females (9.2 million) were victims of identity theft than males (8.3 million) in 2014.
- People in households with an annual income of $75,000 or more had the highest prevalence of identity theft (11 percent), compared to those in all other income brackets.
- Ten percent of identity theft victims reported that the crime was severely distressing, compared to 33 percent of violent crime victims.

The report, *Victims of Identity Theft, 2014* (NCJ 248991), was written by BJS statistician Erika Harrell. The report, related documents and additional information about the Bureau of Justice Statistics' statistical publications and programs can be found on the BJS website at http://www.bjs.gov/.

# # #

The Office of Justice Programs (OJP), headed by Assistant Attorney General Karol V. Mason, provides federal leadership in developing the nation's capacity to prevent and control crime, administer justice, and assist victims. OJP has six components: the Bureau of Justice Assistance; the Bureau of Justice Statistics; the National Institute of Justice; the Office of Juvenile Justice and Delinquency Prevention; the Office for Victims of Crime; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. More information about OJP can be found at http://www.ojp.gov.

Appendix E. Better Business Bureau Top 10 Scams

January 28, 2015
Arlington, VA – Better Business Bureau hears from thousands of consumers and business owners every year about a variety of scams and frauds. Many are new twists on existing scams, but scammers get more sophisticated every year in how they spoof trusted names and how they fool consumers.
While BBB doesn't have specific numbers about how many people were defrauded or for how much, here are the scams we think were most pervasive this past year:

#10 Sweepstakes Scam: You've won a contest! Or the lottery! Or the Publishers Clearinghouse Sweepstakes! All you have to do to claim your prize is to pay some fees or taxes in advance so they can release your prize… This is not a new scam, but it is a perennial problem.

#9 Click Bait Scam: This one takes many forms, but the most notorious of the past year was when the Malaysian Airline plane went missing ("click here for video"). Other click bait schemes use celebrity images, fake news, and other enticing stories to get you to unintentionally download malware.

#8 Robocall Scam: The notorious "Rachel from Cardholder Services" made a resurgence in 2014. This scam claims to be able to lower your credit card interest rates and takes personal information – including your credit card number – and then charges fees to your card.

#7 Government Grant Scam: You get a call saying you've been awarded a government grant for thousands of dollars. It may even mention a program you've heard about in the news. All you have to do to collect your grant is pay a couple hundred in fees by wire transfer or prepaid debit card.

#6 Emergency Scam: This one is sometimes called the "grandparent scam" because it often preys on older consumers. You get a call or email from your grandchild or other relative who was injured, robbed or arrested while traveling overseas and needs money ASAP.

#5 Medical Alert Scam: Another one that preys on older folks. You get a call or a visit from a company claiming a concerned family member ordered you a medical alert device in case you have an emergency. They take your credit card or banking information but you never receive anything.

#4 Copycat Website Scam: You get an email, text message or social media post about a terrific sale or exciting new product. You click through and it looks just like a

popular retailer's site. But when you order, you either get a cheap counterfeit or nothing at all… and now they have your credit card number!

#3 "Are You Calling Yourself?" Scam: Scammers can make a call look like it's coming from anywhere. The latest trick puts *your* number in the Caller ID, which piques your curiosity and gets you to pick up the phone or return the call… and then they've snagged you in whatever scam they are running.

It was almost a tie for the top spot this year, because BBB sees this one every day:

#2 Tech Support Scam: You get a call or a pop-up on your computer claiming to be from Microsoft (or Norton, or Apple) about a problem on your computer. They say if you give "tech support" access to your hard drive, they can fix it. Instead, they install malware on your computer and start stealing your personal information.

And the top **Scam of the Year**, because it's just so terrifying, is:

#1 Arrest Scam: You receive an ominous phone call from someone claiming to be a police officer or government agent (often the IRS in the United States or the CRA in Canada). They are coming to arrest you for overdue taxes or for skipping out on jury duty… but you can avoid it by sending them money via a prepaid debit card or wire transfer. Another variation on this is that you'll be arrested for an overdue payday loan. Whatever the "violation," it's scary to be threatened with arrest, and many people pay out of fear.

Appendix F. Proposal Part I: Rock County Circuit Court / Clerk of Court Operational Data Security Plan

Physical Data Security

Hardcopy – Paper Document Disposal

- E-filing Rule: Documents filed by traditional methods shall be electronically scanned and made part of the official record. The clerk of court may discard the paper copy immediately, notwithstanding SCR 72.03 (3).
- In accordance with SCR E-filing Rule, Rock County Circuit Court personnel will discard all court paper copies by shredding.
- Any documents generated by court personnel (i.e. screen prints) containing personally identifying information (PII) shall be destroyed by shredding.
- Paper documents shall be destroyed daily. If the event time does not permit daily disposal, documents shall be maintained in locked storage area.
- Disposal of all paper files, in accordance with SCR 72.03 shall be shredded. Paper files shall be placed in locked shredding bins provided by Office-Pro. When bins are at capacity, court personnel are to notify Chief Deputy or Court Office Manager for removal and replacement. Office-Pro bins are located in the courthouse basement court vaults, clerk of circuit court office, 5th floor judicial offices, and off-site storage “Building B”.

Electronic Security

Network Security

- Network security will be maintained and managed by the State of Wisconsin Consolidated Court Access System (CCAP) personnel.

User Security

- User security shall be assigned and maintained by the Rock County CCAP Administrators: Chief Deputy and Court Office Manager.
- Users shall use strong CCAP passwords; including a mix of letters, numbers, and characters.
- CCAP-activated screen savers will be activated after a period of user inactivity.
- Users shall refrain from opening emails or downloads from unknown origins.
- Users shall use extreme caution when emailing sensitive data, both internally and externally.

Laptop and Mobile Device Security

- Assigned ‘court’ and ‘clerk’ cellular phones shall be used only for intended purposes only (i.e. interpreter contact).
- Assigned ‘court’ and ‘clerk’ cellular phones shall not leave the premises without prior approval.
- Wireless and remote access through laptops and other mobile devices are assigned and maintained by CCAP and are limited to employees that have a legitimate need to work outside of Rock County Courthouse.
- Employees assigned laptops and other mobile devices shall comply with all CCAP data security standards and make every effort to secure devices at all times to prevent information compromise and theft.

Equipment Security

- Multi-purpose digital copier(s) shall have passcode data security feature, encryption and overwriting features.
- Multi-purpose digital copier(s) hard drives will be removed and wiped at the end of the contract period by Rock County Information Technology.
- Fax machines, when no longer functioning or utilized, shall be relinquished to Rock County Information Technology for proper disposal.
- Stenographer equipment shall meet all CCAP data security standards.

Protocols

- Information compromises and/or security breaches shall be reported immediately to your supervisor.
- Possible ‘scam’ notifications (commonly reported by the public: arrest / jury duty scam) shall be forwarded to immediately to your supervisor.

*The Personal Data Privacy and Security Act of 2009 outlines **personally identifying information (PII)** as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information”.*

Proposal Part II: Privacy, Confidentiality, and Information Security Agreement

As an employee of the Rock County Circuit Court System and a user of the State of Wisconsin Consolidated Court Access System (CCAP), I understand that I am responsible for the security of my user ID (login) and password for which I am granted access. I understand that it is my responsibility to protect my password's confidentiality. I understand that I have the following responsibilities:

• Comply with all CCAP policies.

• Comply with all state statutes, local court rules, and state/county policy requirements.

• Protect CCAP access accounts, privileges, and associated passwords (i.e. not sharing my password).

• Maintain the confidentiality of information to which I am given access privileges.

• Accept accountability for all activities associated with the use of my individual user account and related access privileges.

• Not to change the computer configuration unless specifically approved to do so.

• Not to disable or alter the anti-virus and/or firewall software.

• Not to download, install or run unlicensed or unauthorized software.

• Ensure that my use of CCAP system, and information accessed, stored, or used is restricted to authorized duties or activities.

• Report all suspected security and/or policy violations to my supervisor.

• Report all known privacy violations to my supervisor.

I understand that where I have access to or use of personally identifiable information (PII), sealed and/or confidential records, additional protections are expected.

I understand that I must maintain and safeguard the confidentiality of personally identifying information (PII) and all Rock County Circuit Court sealed and/or confidential

information accessed or obtained in the performance of my authorized duties or activities. I will not access, use, and/or disclose personally identifying information (PII), sealed and/or confidential information for any purpose other than the performance of authorized activities or duties. I will limit my access, use and disclosure to the minimum amount of information necessary to perform my authorized activity or duty.

I will safeguard all personally identifying information (PII), sealed and/or confidential information by holding it in the strictest confidence and by refusing to allow others to access information unless my authorized activities require that I do so. In such cases, I will disclose or allow access only to individuals having appropriate authority to access, receive and use such information.

I understand that my access to CCAP system that contains personally identifying information (PII), sealed and/or confidential information may be monitored to assure appropriate access and compliance with system integrity. I understand that authorized use carries with it the responsibility to follow all federal and state statutes, local court rules, State of Wisconsin and Rock County Circuit Court policies and procedures that govern record management, information and data security, record retention, and confidentiality.

I understand that failure to comply with the above Privacy, Confidentiality, and Information Security agreement may result in disciplinary action up to and including denial of access to information and termination of my employment with Rock County Circuit Courts / Clerk of Circuit Courts.

I have been given access to all of statutes, rules, policies and procedures that govern Rock County Circuit Courts / Clerk of Circuit Courts.

E-filing / Redaction:

http://wicourts.gov/ecourts/docs/redactionproposed.pdf

Record Retention:

http://courtnet.wicourts.gov/SearchCourtnet?query=retention

Exhibit Management:

http://courtnet.wicourts.gov/SearchCourtnet?query=exhibit

Facilities Security:

http://wicourts.gov/sc/scrule/DisplayDocument.pdf?content=pdf&seqNo=79810

Record Management:

http://courtnet.wicourts.gov/policies/docs/retentionbrochure.pdf

Model Recordkeeping:

http://courtnet.wicourts.gov/policies/modelrecord.htm

Confidential Records:

http://courtnet.wicourts.gov/policies/docs/confidentialitystatutelist1015.pdf

Disaster Recovery:

http://courtnet.wicourts.gov/policies/docs/disasterrecovery.pdf

Customer Service:

http://courtnet.wicourts.gov/education/Walking_the_Line/index.html

By signing this Agreement, I understand and agree to abide by the conditions imposed above.

_____ _____

Employee Date

_____ _____

Supervisor Date