

- **Internet records.** Effective September 1, 2008, the bill prohibits any public office or person responsible for a public office's public records from posting on the Internet or the public office's web site any document that contains an individual's Social Security number, without otherwise redacting the information. Costs to obtain software that would redact, encrypt, or truncate Social Security numbers from public records found online may vary widely by agency based on the solution employed. For instance, costs for state agencies to remove any state documents that contain Social Security numbers from public access on the Internet would likely be minimal, but purchasing such solutions as automated redaction systems would pose additional costs, which could be in the tens of thousands of dollars.
- **Redaction requests.** It is likely that there would not be a significant additional workload for state agencies to review and redact the addresses or personal information for persons making redaction requests under the bill. Any additional cost will depend upon the number of persons making such requests, the agencies to which the requests are made, and the number and type of records posted online by state agencies that would have to be redacted.
- **Chief Information Security Officer.** In addition to statutorily creating the Chief Privacy Officer position in the Department of Administrative Services (DAS), the bill creates a new position, the Chief Information Security Officer (CISO), to assist each state agency with the development of an information technology security strategy. It would result in new annual payroll costs of up to \$125,000 for the Office of Information Technology within DAS. Based on the September 1, 2008 effective date in the bill, the CISO position's payroll costs may only be up to \$104,000 in FY 2009.
- **Identity fraud enforcement grants.** The bill stipulates that the Office of Criminal Justice Services in the Department of Public Safety is to make one-time state funding grants available to local law enforcement agencies to enable local law enforcement to develop the capabilities to enforce identity fraud crimes. The bill does not specify a funding source for the grants or the maximum amount that may be allocated.
- **Security freeze enforcement.** The bill gives the Attorney General authority to enforce the provisions related to security freezes, including the authority to bring a civil action for appropriate relief, including a temporary restraining order, injunction, and civil penalties if it appears that a consumer credit reporting agency has failed or is failing to comply with the bill's provisions. It is assumed that the number of actions filed will be a fairly small number on an annual basis. If such actions are filed, there may be an increase in expenses from the Consumer Protection Enforcement Fund (Fund 6310) for investigation and litigation expenses as well as a gain in revenue to that fund from any awards to the Attorney General for costs associated with the actions and civil penalties.
- **Secretary of State filings.** The bill prevents the Secretary of State (SOS) from accepting certain documents for filing or recording if the document includes any individual's social security number or federal tax identification number. SOS may have to spend additional money on postage to return some documents that still have the numbers on them, but it would likely be no more than a minimal amount annually.

Local Fiscal Highlights

LOCAL GOVERNMENT	FY 2008	FY 2009	FUTURE YEARS
Counties and Municipalities			
Revenues	Potential gain from identity fraud grants and court cost and filing fee revenue	Potential gain from identity fraud grants and court cost and filing fee revenue	Potential gain from identity fraud grants and court cost and filing fee revenue
Expenditures	Potential increase for redaction software; potential minimal increase to perform redactions and to adjudicate civil and criminal cases; potential minimal increase in county recorder postage	Potential increase for redaction software; potential minimal increase to perform redactions and to adjudicate civil and criminal cases; potential minimal increase in county recorder postage	Potential increase for redaction software; potential minimal increase to perform redactions and to adjudicate civil and criminal cases; potential minimal increase in county recorder postage
Townships			
Revenues	Potential gain from identity fraud grants	Potential gain from identity fraud grants	Potential gain from identity fraud grants
Expenditures	Potential increase for redaction software; potential minimal increase to perform redactions	Potential increase for redaction software; potential minimal increase to perform redactions	Potential increase for redaction software; potential minimal increase to perform redactions

Note: For most local governments, the fiscal year is the calendar year. The school district fiscal year is July 1 through June 30.

- **Internet records.** Costs for local governments to obtain software that would redact, encrypt, or truncate Social Security numbers from public records found online may vary widely by political subdivision based on the solution employed. For instance, costs to remove any documents that contain Social Security numbers from public access on the Internet would likely be minimal, but purchasing automated redaction systems would pose additional costs, which could be in the tens of thousands of dollars.
- **Redaction requests.** For local governments, redacting addresses or personal information for persons making redaction requests under the bill would appear to impose no more than a minimal cost.
- **County recorder filings.** The bill prohibits preparers of documents recorded by county recorders from including personal information in documents filed for recording. County recorders may have to spend additional money on postage to return some documents that still have personal information on them, but it would likely be no more than a minimal amount annually.
- **Local civil justice costs – security freeze enforcement.** It is expected that the number of cases filed by either the Attorney General or consumers for violations of the bill's provisions concerning security freezes would not be significant in terms of a county common pleas court's or municipal court's caseload. However, it is possible that this bill may minimally increase adjudication costs for county and municipal courts over what they would be absent the bill's enactment. These additional costs may be offset through court cost and filing fee revenue.

- **Extended statute of limitations.** The bill enacts a special statute of limitations for criminal prosecutions and civil actions against identity fraud. This opens the possibility of additional county and municipal court cases related to identity theft cases. The extended statute of limitations may increase local criminal and civil justice caseloads and thus, the expenditures related to prosecuting and adjudicating identity fraud cases, but the additional amount is expected to impose no more than a minimal cost to county and municipal courts. Any additional cost may be mitigated through court cost, filing fee, and fine revenue.
 - **Identity fraud enforcement grants.** The bill stipulates that the Office of Criminal Justice Services in the Department of Public Safety is to make one-time state funding grants available to local law enforcement agencies to enable local law enforcement to develop the capabilities to enforce identity fraud laws. The bill does not specify a funding source for the grants or the maximum amount that may be allocated. Therefore, the revenue gain to local law enforcement agencies from the grants is unknown.
-

Detailed Fiscal Analysis

Overview

This bill addresses issues connected with identity theft and fraud in many different aspects. It modifies statutes concerning public records to require public offices to redact, encrypt, or truncate Social Security numbers found on any document posted on the Internet and to maintain a database or list that includes the name and date of birth of all public officials or employees elected to or employed by that public office that must be made available upon a public records request. Further, the bill allows individuals and certain public safety, justice and corrections employees to request that a public office redact personal information or addresses, respectively, from documents made available to the general public online.

Among other changes, the bill also allows a consumer to place a security freeze on the consumer's credit report and requires the Attorney General to enforce the security freeze provisions. Beyond those measures, the bill contains provisions aimed at preventing identity theft, such as prohibiting the Secretary of State from accepting certain documents for filing or recording if they include any individual's Social Security numbers or federal tax identification numbers and county recorders from accepting documents for filing or recording if they include any individual's personal information. Additionally, the bill requires the Office of Criminal Justice Services to make state funding grants available to local law enforcement agencies for enforcement of identity fraud laws. Finally, the bill enacts a special statute of limitations for criminal prosecutions and civil actions against identity fraud.

Public records provisions

Internet public records redaction

Effective September 1, 2008, the bill prohibits any public office or person responsible for a public office's public records from posting on the Internet any document that contains an individual's Social Security number (SSN) unless the SSN is redacted, encrypted, or truncated. All records that contain SSNs posted before the bill's effective date must also have that information redacted, encrypted, or truncated. The bill clarifies that these provisions do not apply to documents that are only accessible online with a password.

According to an official in the Office of Information Technology (OIT), while software exists to redact Social Security numbers, there are likely few agencies currently utilizing such software. It may be that state agencies and local governments would need to purchase software and/or hardware to redact or otherwise obscure Social Security numbers if they were to opt to redact such information from public documents so that they would remain accessible through the Internet.

The costs for such an initiative are uncertain as a variety of solutions may be employed to restrict Social Security numbers found online or to perform redactions. Generally, new costs for most state agencies and local governments to remove documents containing Social Security numbers from public access on the Internet would appear to be minimal. As an alternative, software such as Adobe Acrobat may be used to perform manual redactions on PDF files (the format often used to post documents online), the cost of which could be minimal but would depend on the number of copies needed.¹ Automated solutions, such as that used by the Secretary of State's office (SOS) to redact Social Security numbers from Uniform Commercial Code (UCC) documents can be in the tens of thousands of dollars. SOS's current contract with Extract Systems for I.D. Shield software is for \$48,000, which includes the procurement of two servers (\$4,000), on-site installation (\$6,000) and the capability to redact up to 2.2 million images.

Redaction requests

The bill allows individuals to request that a public office redact personal information (defined as an individual's Social Security number, federal tax identification number, driver's license number or state identification number, or various financial account numbers) from any record made available to the general public online. The request must be in writing, specify the personal information to be redacted, and provide any information that identifies the location of the personal information on the document. Public offices have five business days to perform the redaction if the redaction is practicable or must notify the person within five business days and explain why the redaction is not practicable.

Similarly, the bill permits persons in eight specific vocations (peace officer, parole officer, prosecuting attorney, assistant prosecuting attorney, correctional employee, youth services employee, firefighter, and EMT) to request a public office (other than a county auditor) to redact the person's address from any record made available to the general public online. The same timelines for the public office to perform redactions or to explain why the redaction cannot be performed for individuals also apply to requests made by persons in the eight specific vocations. The Attorney General must develop forms for such persons to request redactions. Any costs associated with developing these forms would likely be negligible.

Under current law, residential and familial information (which, among other information, includes the residential street address, residential telephone number, bank account or other financial information, and social security number) of the persons in the eight vocations listed in the bill is not considered public record, so it is uncertain how many persons in such vocations would opt to request a redaction permitted under the bill.

¹ A single copy of Adobe Acrobat Professional 8.0 and optional redaction software "plug-ins" can cost several hundred dollars depending on the vendor.

According to the Department of Administrative Services (DAS), there is little personal information on most state forms that is not already redacted prior to release. Thus, it is likely that there would not be a significant additional workload for state agencies to review documents to redact the addresses or personal information for the persons making the request. For local governments, these provisions would appear to impose no more than a minimal cost. Redaction costs for most municipalities and villages would likely be negligible, as, according to the Ohio Municipal League, most of these entities' public records do not include much personal information. Overall, any additional cost will depend upon the number of persons making such requests, the public offices to whom the requests are made, and the number and type of records posted online by the public office that would have to be redacted.

Public officials and employees information

The bill requires each public office to maintain a database or list that includes the name and date of birth of all public officials or employees elected to or employed by the public office that must be made available upon a public records request. It is likely that the development and maintenance of such a list or database would pose only a negligible cost at most.

Security freezes

The bill enables a consumer to place a security freeze on the consumer's credit report beginning on September 1, 2008. A security freeze is defined to be a restriction placed in a consumer's credit report at the request of the consumer that prohibits a consumer credit reporting agency from releasing all or part of the consumer's credit report or any information derived from the consumer's credit report relating to the extension of credit without express authorization of the consumer. Over 30 states have enacted similar legislation.

The bill allows a consumer credit reporting agency to charge a consumer a fee of \$5 for placing the security freeze, removing or temporarily lifting the freeze, and providing a new or reissuing a personal identification number (PIN). There would be no charge for placement of a security freeze for victims of identity fraud. The consumer credit reporting agency would collect any fees charged.

Enforcement by the Attorney General

The bill gives the Attorney General authority to enforce the provisions related to security freezes, empowering this office to conduct investigations, based on complaints or the Attorney General's own inquiries, concerning consumer credit reporting agencies that are believed to be failing to comply with the bill's requirements concerning security freezes.

In addition, the bill also gives the Attorney General authority to bring a civil action in a court of common pleas for appropriate relief, including a temporary restraining order, injunction, and civil penalties if it appears that a consumer credit reporting agency has failed or is failing to comply with the bill's provisions. If a consumer credit reporting agency has intentionally or recklessly failed to comply with the bill's requirements concerning security freezes, a court of common pleas must impose a civil penalty on the consumer credit reporting agency of up to \$2,500 for each instance that the consumer credit reporting agency fails to comply. Consumer credit reporting agencies found in noncompliance are liable to the Attorney General for the

Attorney General's costs in conducting the investigation and bringing the action. All civil penalties are to be deposited into the Consumer Protection Enforcement Fund (Fund 6310).

It is uncertain how often the Attorney General would file such actions, but it is assumed that it will be a fairly small number on an annual basis given that participation in the states that have had security freezes available to consumers for several years has been low and such an action would likely be a last resort. If such actions were filed, there may be an increase in expenses from the Consumer Protection Enforcement Fund or the GRF as well as a gain in revenue to the Consumer Protection Enforcement Fund from any awards of investigation and litigation costs and civil penalties.

Consumer actions

The bill also allows the consumer to file a civil action against the consumer credit reporting agency if the agency does not place a security freeze requested in the allotted times in the bill or changes official information in a credit report without notifying the consumer within 30 days of the change. Damages are limited to the greater of actual damages or damages between \$100 and \$1,000, any punitive damages the court allows, and court costs with reasonable attorney's fees. The bill also makes consumer credit reporting agencies that are negligent in the above activities or that allow another person to obtain a consumer's credit report liable for actual damages, court costs, and reasonable attorney's fees. If the court finds that a civil action was brought in bad faith or for harassment, the consumer credit reporting agency must be awarded reasonable attorney's fees in relation to the work expended in responding to the civil action. Consumers must bring a civil action within two years after the date of discovery by the plaintiff of the above violations or five years after the violations above occur, whichever is earlier.

Local civil justice costs

It is uncertain how many civil cases the Attorney General will file in enforcing this bill or consumers may bring in seeking remedies, but it is expected that the number would not be significant in terms of a county common pleas court's or municipal court's caseload. However, it is possible that this bill may minimally increase adjudication costs for county and municipal courts over what they would be absent the bill's enactment. These additional costs may be offset through court cost and filing fee revenue.

Other identity theft prevention provisions

Secretary of State – social security number prohibitions

The bill prevents the Secretary of State (SOS) from accepting certain documents for filing or recording if the document includes any individual's social security number or federal tax identification number. If a document contains such information and SOS refuses to accept the document, SOS or the person filing the document may immediately redact the information from the document. An official in the SOS's Business Services Division indicated that staff already review filings for social security and federal tax identification numbers, meaning that there would likely be no extra work to proofread documents. However, it may be that SOS would have to spend money on postage to return some documents that still have the numbers on them. Such new costs would likely be no more than a minimal amount.

County recorders – personal information prohibitions

The bill prohibits preparers of documents recorded by county recorders from including personal information in documents filed for recording. A county recorder's office could incur new work due to the inevitable extra proofreading of documents for personal information, rejecting and returning those that still have the information on them, and then reviewing the corrected documents. County recorders currently prohibit the inclusion of SSNs on documents filed for recording as a result of Sub. H.B. 279 of the 126th General Assembly. The Ohio County Recorders Association indicated that there are not a significant number of recorded documents containing federal tax identification numbers, driver's license numbers, or the various financial account numbers. Therefore, while it is doubtful that the staff in the recorder's office would work overtime hours to do this because the work would likely be completed within their regular hours, it may be that the recorder's office would have to spend money on postage to return some documents.

LSC fiscal staff research reveals that, of the documents received in the recorder's office, approximately 30%-50% come by mail and 50%-70% are brought in person. Those that are received by mail often include a stamped, self-addressed envelope for the return of documents. One recorder's office estimated that as many as 95% of mailed documents are accompanied by a stamped, self-addressed envelope for the return of materials, whereas documents that are delivered by person may or may not be accompanied by a stamped, self-addressed envelope. Some recorders make a requirement that stamped return envelopes must be supplied by the preparer at the time documents are filed.

In cases where no return envelope is provided, the recorder incurs costs to return documents to the sender. The minimum postage on documents that the recorder usually handles and files is 50-60 cents. Documents for which the recorder incurs postage expenses constitute a small fraction of the total volume of documents that are handled.

County auditors – tax list removal requests

Each year, county auditors are required to compile a general tax list of real and public utility property in their county by listing all parcels in the county containing the names of the persons, companies, firms, and so forth the real property has been listed under. The bill permits persons in the eight public safety, justice and corrections vocations noted above to request that a county auditor replace that person's name from the general tax list of real and public utility property and its duplicate with the person's first and last initials as the name of the person appears on the deed. The county auditor is to act within five business days if the request is practicable. If the request is not practicable, the county auditor must notify the requestor within five business days and explain why the request is not. The bill also prohibits county auditors from charging a real property conveyance fee to a person making such a request.

The Ohio County Auditors Association indicated that, generally, replacing a person's name with that person's initials would not be burdensome for county auditors. The process would likely only involve entering the change in a computer. Therefore, additional expenses for county auditors, if any, would appear to be negligible.

Office of Information Technology – new payroll costs

The bill requires the Director of OIT to (1) establish policies and procedures for the security of personal information maintained and destroyed by state agencies, (2) employ a Chief Information Security Officer (CISO) who is responsible for the implementation and coordination of the above policies and procedures in all state agencies, and (3) employ a Chief Privacy Officer (CPO) who is responsible for advising OIT and state agencies when establishing policies and procedures for the security of personal information and developing education and training programs regarding the state's security procedures. OIT currently employs a person in the CPO position (classified as a Deputy Director 3 with annual payroll costs of \$110,000 maximum), so there would be no new personnel costs brought about by this position. However, new payroll costs would be brought about through the creation of the CISO position. OIT reported that the CISO would be classified as something similar to a Data Systems Administrator with new payroll costs of up to \$125,000 annually. The higher compensation for the CISO is attributable to the technical expertise required and private sector demand for a qualified individual in that role. Payroll costs for the CISO would likely be paid from the IT Governance Fund (Fund 2290), which is funded by charges to state agencies for IT services. Based on the September 1, 2008 effective date in the bill, the CISO position's payroll costs may only be up to \$104,000 in FY 2009.

Concerning personal information security policies, while there is not one single policy addressing the subject, there are many IT security policies, standards, and bulletins in place giving guidance on that issue. One such document, IT Bulletin No. ITB-2007.02, establishes guidelines for agencies in handling sensitive data. This bulletin and other IT policies may be found online at <http://www.oit.ohio.gov/IGD/policy/OhioITPolicies.aspx>.

The CISO is tasked with assisting each state agency with the development of an information technology security strategy and reviewing that plan. Each state agency must submit such a plan to OIT and prepare or have prepared a privacy impact assessment for any new information technology data system that the agency intends to implement prior to the actual implementation of that system. As of this writing, it is uncertain what the costs may be for state agencies to prepare the privacy impact assessment and develop an information technology security strategy.

Criminal Justice Services grants

The bill stipulates that the Office of Criminal Justice Services (OCJS) in the Department of Public Safety is to make one-time state funding grants available to local law enforcement agencies to enable local law enforcement to develop the capabilities to enforce identity fraud laws. These grants would likely be for updated computer technology or staff training in the area of identity theft law enforcement. The authority to issue grants under the bill expires two years after the bill's effective date. The bill does not specify a funding source for the grants or the maximum amount that may be allocated by OCJS. Consequently, the revenue gain to local law enforcement agencies from the grants is unknown.

Extended statute of limitations for identify fraud

The bill enacts a special statute of limitations for criminal prosecutions and civil actions against identity fraud. This opens the possibility of additional county and municipal court cases related to identity theft cases. For instance, the bill includes an increase in the statute of

limitations in civil identity theft cases from four years to five years and extends the statute of limitations in criminal identity theft cases an extra five years from discovery. According to data from the Franklin County Municipal Court and Montgomery County Common Pleas Court, the number of identity theft offenders is likely small for any given county. For example, Franklin County reported 69 charges filed for identity falsification and Montgomery County reported filing 30 criminal cases of identity fraud, both in CY 2006. These statistics are comparable to those for CY 2005, when Franklin County reported 63 identity falsification charges and Montgomery County reported 39 identity fraud criminal cases. Therefore, while the extended statute of limitations may increase local criminal and civil justice caseloads and thus, the expenditures related to prosecuting and adjudicating identity fraud cases, the additional amount is expected to impose no more than a minimal cost to county and municipal courts. Any additional cost may be mitigated through court cost, filing fee, and fine revenue.

Identity theft complaints

Another source of information concerning the prevalence of identity theft is a data clearinghouse maintained by the Federal Trade Commission (FTC), which logs complaints of identity theft and tracks the location and the types of fraud and identity theft. As the reporting process is voluntary, the FTC's numbers do not provide a complete picture of the number of identity theft complaints that reach local police departments. For the one-year time period covering January 1, 2007 through December 31, 2007, the FTC recorded 7,178 total complaints of identity theft in Ohio. The table below summarizes the number and types of identity fraud complaints received by the FTC in CY 2007. Note that 15% of identity fraud complaints from Ohio victims include more than one type of identity theft. Therefore, the figures below represent the number of identity theft complaints by type (which will add to more than 7,178), not the number of identity theft victims.

FTC Identity Fraud Complaints, CY 2007	
Type of Identity Fraud Complaint	Number
Phone or Utilities Fraud	2,034
Other Identity Theft*	1,753
Credit Card Fraud	1,631
Bank Fraud	889
Government Documents/Benefits Fraud	692
Attempted Identity Theft	410
Employment Related Fraud	406
Loan Fraud	281

*Other identity theft includes Internet/e-mail fraud, medical fraud, insurance fraud, and so on.

LSC fiscal staff: Jason Phillips, Budget Analyst
HB0046SP/rh