

- **Internet records.** Effective July 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 various pieces of personal information, such as a person's social security number, without otherwise redacting the information. Costs to obtain software that would redact, encrypt, or truncate personal information 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 personal information 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.
- **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 given the low rate of participation in states that have had security freezes available to consumers for several years. If such actions are filed, there may be an increase in expenses from the Consumer Protection Enforcement Fund (Fund 631) 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.
- **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.
- **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 2007	FY 2008	FUTURE YEARS
Counties and Municipalities			
Revenues	- 0 -	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	- 0 -	Potential increase for redaction software and to adjudicate civil and criminal cases	Potential increase for redaction software and to adjudicate civil and criminal cases
Townships			
Revenues	- 0 -	Potential gain from identity fraud grants	Potential gain from identity fraud grants
Expenditures	- 0 -	Potential increase for redaction software	Potential increase for redaction software

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

- **Internet and electronic records.** Costs for local governments to obtain software that would redact, encrypt, or truncate personal information 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 personal information from the 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.
- **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 any personal information found on any document posted on the Internet or public office's web site and to maintain a database or list that includes the name and date of birth of public officials and employees that must be made available upon request as a public record. 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 these 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, requiring policies and procedures to be in place for the security of personal information maintained and destroyed by the state. 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 July 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 a person's personal information (defined as a person's Social Security number, federal tax identification number, driver's license number or state identification number, or certain financial account numbers) unless that information is redacted, encrypted, or truncated. All records that contain personal information posted before the bill's effective date must also have that information redacted, encrypted, or truncated.

According to an official in the Office of Information Technology (OIT), while software exists to redact personal information such as that listed above in order to meet the redaction requirements in the bill, 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 the personal information listed above 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 personal information found online or to perform redactions. Generally, new costs for most state agencies and local governments to remove documents containing personal information 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.

Public officials and employees information

The bill requires public offices to maintain a database or list that includes the name and date of birth of public officials and employees that must be made available upon request as a public record. 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 in FY 2009. 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 various fees for placing the security freeze, removing or temporarily lifting the freeze, and providing a new or reissuing a personal identification number (PIN). The table below summarizes the fees included in the bill. The consumer credit reporting agency would collect any fees charged.

Consumer Credit Reporting Agency Security Freeze Fees	
Action	Fee
Initial Placement of Security Freeze (no charge for victims of identity fraud)	\$5 maximum
Removal or Temporary Lifting of Security Freeze for Specific Period of Time	\$5 maximum
Removal or Temporary Lifting of Security Freeze for Specific Creditor	\$5 maximum
Reissuance of Personal Identification Number (PIN)	\$5 maximum

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.

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.

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 631).

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 (Fund 631) or the GRF as well as a gain in revenue to that 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 between \$100 and \$1,000, any punitive damages the court allows, and court costs with reasonable attorney's fees as determined by the court. 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.

Office of Information Technology – Chief Privacy Officer

The bill requires the Director of OIT to (1) establish policies and procedures for the security of personal information maintained and destroyed by the state and (2) employ a Chief Privacy Officer (CPO) who is responsible for the implementation and coordination of the above policies and procedures in all state agencies. OIT currently employs a person in the CPO position, so there would be no new personnel costs brought about by this provision. Additionally, the CPO noted that while there is not one single policy addressing the security of personal information, there are many IT security policies standards, and bulletins in place giving guidance on those issues. 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>.

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, 2006 through December 31, 2006, the FTC recorded 6,878 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 2006. Note that 17% 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 6,878), not the number of identity theft victims.

Type of Identity Fraud Complaint	Number
Other Identity Theft*	1,788
Phone or Utilities Fraud	1,720
Credit Card Fraud	1,651
Bank Fraud	1,032
Government Documents/Benefits Fraud	550
Employment Related Fraud	413
Attempted Identity Theft	413
Loan Fraud	275

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

LSC fiscal staff: Jason Phillips, Budget Analyst

SB0006S2/lb