HB 1120

Department of Legislative Services

Maryland General Assembly
2009 Session

FISCAL AND POLICY NOTE

House Bill 1120 (Delegate Lee, *et al.*)
Economic Matters

Social Security Numbers - Prohibited Uses

This bill prohibits a person from printing, storing, or using an individual's Social Security number (SSN) in specified circumstances. The bill also prohibits a unit or instrumentality of the State, or a political subdivision of the State, from using or requiring the use of an individual's SSN on a public record.

Fiscal Summary

State Effect: The bill's provision related to State government primarily codify current practice. If the Consumer Protection Division of the Office of the Attorney General receives fewer than 50 complaints stemming from this bill, the additional workload can be handled with existing resources.

Local Effect: The bill's provisions related to local government primarily codify current practice.

Small Business Effect: Potential minimal.

Analysis

Bill Summary: A "person" is defined as an individual, corporation, business trust, estate trust, partnership or association, or similar entity, but does not include a unit of State or local government. The bill prohibits a person from printing or storing an individual's SSN on (1) a card required for the individual to access products or services; or (2) an identification card issued to the individual. A person is further prohibited from using an individual's SSN for commercial gain, and unless required by federal law, may not

include an individual's SSN on a document used for any Medicare or Medicaid program. A person cannot require an individual to use the individual's SSN as an access code.

Although a person is allowed to include an individual's SSN in an application, form, or document sent by mail, e-mail, or facsimile as part of an application process, to modify a current contract or policy, or to confirm the accuracy of the individual's SSN, a person may not include an individual's SSN on any credit card application documents.

Current Law: The Social Security Number Privacy Act, codified in the Commercial Law Article of the Annotated Code of Maryland, prohibits a person from:

- publicly posting or displaying an individual's SSN;
- printing an individual's SSN on a card required for the individual to access products or services;
- requiring an individual to transmit the individual's SSN over the Internet unless the connection is secure or the SSN is encrypted;
- initiating the transmission of an individual's SSN over the Internet unless the connection is secure or the SSN is encrypted; and
- requiring an individual to use the individual's SSN to access an Internet web site, unless a password, unique personal identification number, or other authentication device is also required to access the web site.

Unless required by State or federal law, a person may not:

- print an individual's SSN on any material that is mailed to the individual;
- include an individual's SSN in any material that is electronically transmitted to the individual, unless the connection is secure or the individual's SSN is encrypted; or
- include an individual's SSN in any material that is transmitted by facsimile to the individual, with specific exceptions.

The Act does not apply to the collection, release, or use of an individual's SSN as required by State or federal law and does not prohibit a person from requesting an individual's SSN in an application, form, policy, or other similar document.

Background: In the 2007 session, the General Assembly adopted the Personal Information Protection Act (PIPA) in response to escalating instances of loss or theft of personal information held by government agencies or private data collection companies. PIPA requires any business that retains consumer records to notify a State resident if his or her personal information has been compromised. According to the Attorney General's Office, between January 15, 2008 and February 2, 2009, the personal information of

406,459 State residents was compromised in a total of 237 corporate security breaches. These security breaches ranged from the theft of corporate laptops to the hacking of corporate networks, and included the dissemination of personal information such as:

- names, addresses, e-mail accounts, dates of birth, and SSNs;
- employee identification and tax identification numbers;
- credit card, checking, debit, and bank account numbers; and
- personal financial records, medical insurance records, and other health-related information.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Carroll, Harford, and Montgomery counties; Office of the Attorney General (Consumer Protection Division); Department of Budget and Management; Department of Health and Mental Hygiene; Department of Labor, Licensing, and Regulation; Maryland Department of Transportation; Department of Legislative Services

Fiscal Note History: First Reader - March 2, 2009
ncs/ljm

Analysis by: Jason F. Weintraub

Direct Inquiries to:
(410) 946-5510
(301) 970-5510