Identity Theft: Start Protecting Your Community's Personal Information

Whether it's a lost thumb drive, a misplaced report or a computer network infected with malicious software, identity theft is a growing problem in Massachusetts and across the country. All too often we hear horror stories of organizations inadvertently exchanging sensitive information or losing vital records. The media now regularly reports on the loss of personal information by businesses, nonprofits and government agencies alike.

Data breeches can not only cost hundreds of thousands of dollars, but result in lost productivity as staff deal with resolving the issue. In the private sector, customers can quickly lose confidence in the ability of an organization to protect vital information, and take their business elsewhere.

In the public sector, cities and towns are not immune. Identity theft poses a serious problem that can damage the credibility of local government. Some recent reports of identity theft impacting Massachusetts municipalities include:

> An email with the social security numbers, names, and employee identification numbers was accidentally sent to department heads. Some of those emails were automatically forwarded to personal accounts and handheld devices.
>
> An envelope containing the social security numbers, addresses and dates of birth of individuals was mailed to a government agency. When it arrived, the envelope was opened and the contents were missing.
>
> A hacker infected a computer with a virus that tracked the keystrokes including security codes and passwords entered by an official. The information gathered was then used to transfer a considerable amount of funds overseas.

There is no question that cities and towns need to make a conscious effort to invest in methods that protect the public and the municipality when it comes to securing personal information. Examples of personal information include a resident's name in combination with a social security number, driver's license number or financial account information such as bank account or credit card numbers.

Massachusetts General Law (M.G.L.) Chapters 93, 93H and 93I establish comprehensive identity theft prevention measures for business and governmental entities. Although municipalities are exempt from certain regulations promulgated by the state as a result of these laws (201 CMR 17.00), other provisions relative to securing personal information apply

to cities and towns. Specifically, M.G.L. c. 93H includes prompt disclosure requirements when personal information is lost or stolen, while M.G.L. c. 93I sets standards for the disposal of records containing personal information.

So what can be done? To answer this, we outline a process for municipalities to begin protecting confidential information. This is by no means intended to be a comprehensive solution, but includes some immediate steps that cities and towns should take to identify and secure personal information. Also, at the end of this article we provide links to outside resources that provide additional information on implementing preventative identity theft measures.

1. *Designate a Point Person* – First, it is important to determine who will spearhead the initiative and coordinate the city or town's response to protecting personal information. The team leader will be responsible for coordinating access and information gathering among the various departments. The individual should be technically savvy, be able to communicate effectively and be comfortable working with stakeholders from across the organization.

2. *Assemble a Team* – Second, a team of no more than seven members should be formed with the responsibility to collect information and develop a security protocol. We suggest that representatives include someone from the information technology, human resources, finance, legal, and executive offices. Team members should become familiar with identity theft and the level of risk involved.

3. *Identify Personal Information* – Third, the team should compile a written inventory of personal information contained in municipal records. This comprehensive review will determine what constitutes personal information and where it resides within the town. This investigation should identify personal data in both paper and electronic format used by and/or stored by the municipality. Remember, in today's data driven world even photocopy machines store information locally on hard drives.

   Once complete, this document will be used to illustrate the magnitude of risk involved, and be incorporated as part of the overall security policy.

4. *Develop a Security Protocol* – Next, the team should develop, implement, maintain and monitor a comprehensive written security protocol to protect the community's personal information. A plan should include specific and clearly identifiable requirements for protecting confidential data maintained by a department. Although a number of policies are widely circulated on the web, a security plan generally addresses the collection of information, record access, controls, record retention and destruction, physical security, training, and reporting. A final work product should answer any questions related to the protection of personal information within the

municipality. At the end of this article we provide a link to a sample identity theft policy.

5. *React to a Breach* – Lastly, your city or town must react swiftly, and not hesitate to request outside assistance, if personal information is accidentally disclosed or deliberately stolen. We suggest that the team convene to complete an initial assessment of the breach, identifying how and what information might be affected.

   More importantly, however, the team must begin the process of notifying those who might be impacted, so they can begin steps to monitor their accounts for any irregularities. Under M.G.L. municipal officials have the legal obligation to notify any resident affected by the release of personal information, as well as the attorney general and the director of consumer affairs and business regulations.

   Once the team is confident that appropriate steps have been taken to identify, notify and resolve the issue, we recommend it complete a review to determine how future breaches can be prevented and what additional measures may be warranted.

To better understand identity theft, the potential impact to your community, and ways to assist your city or town in protecting confidential information, we provide the following links.

M.G.L. c. 93H: www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h

M.G.L. c. 93I: www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93I/

Department of Revenue, City & Town: http://www.mass.gov/dor/docs/dls/publ/ct/2008/may08.pdf. Link includes a May 2008 article on Identity Theft Prevention by Gary A. Blau, Esq. Municipal Finance Law Bureau.

United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov/cas/tips/. Link includes general information about cyber security, including protecting passwords, understanding anti-virus software and firewalls, as well as recognizing, avoiding and preventing threats.

Multi-State Information Sharing and Analysis Center (MS-ISAC): www.msisac.org/localgov/. Link provides a whole host of resources including guidelines for backing up information, internet and acceptable use policy templates and getting started guides.

Commonwealth of Massachusetts Information Technology Division: www.mass.gov/itd. Link offers various templates, and an information security policy guide