File #: Int 0140-2004, **Version:** A

Int. No. 140-A

By Council Members Reed, Brewer, Gerson, Gioia, James, Nelson, Quinn, Addabbo, Liu, Gentile, Koppell, Monserrate, Weprin and The Public Advocate (Ms. Gotbaum)

A Local Law to amend the administrative code of the city of New York, in relation to requiring city agencies to notify consumers in the event of a security breach of personal identifying information.

Be it enacted by the Council as follows:

Section One. Legislative declaration. The Council finds that acts of identity theft are plaguing New Yorkers. Federal Trade Commission statistics indicate that identity theft has become the single most common consumer fraud complaint in the nation. New York City residents are as likely to be victimized by identity theft as the citizens of many cities within the United States.

The Council finds that identity thieves often gain control of victims' sensitive personal information by hacking into computers or otherwise violating the security of data systems. When such unauthorized persons acquire individuals' personal information, they are able to access bank accounts, take control of credit cards, and defraud unsuspecting victims. The Council thus finds that one of the most effective ways to curtail identity thieves is to inform would-be victims that the security of their sensitive personal information has been violated; individuals can then take the steps necessary to regain control of their privacy and finances.

Accordingly, the Council finds it necessary to require City agencies to inform individuals whenever there has been a breach of security with respect to sensitive personal information. Agencies can best serve New Yorkers by making such disclosures expeditiously, while acting in accordance with the procedures of the New York City Police Department and other legitimate law enforcement agents.

§2. Title 10 of the administrative code of the city of New York is amended by adding a new chapter 5, to

read as follows:

CHAPTER 5

DISCLOSURE OF SECURITY BREACH

§ 10-501 Definitions.

§ 10-502 **Agency disclosure of a security breach.**

§ 10-503 Disposal of personal identifying information.

§10-501 **Definitions** . For the purposes of this chapter,

a. The term "personal identifying information" shall mean any person's date of birth, social security number, driver's license number, non-driver photo identification card number, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person. This term shall apply to all such data, notwithstanding the method by which such information is maintained.

b. The term "breach of security" shall mean the unauthorized disclosure or use by an employee or agent of an agency, or the unauthorized possession by someone other than an employee or agent of an agency, of personal identifying information that compromises the security, confidentiality or integrity of such information. Good faith or inadvertent possession of any personal identifying information by an employee or agent of an agency for the legitimate purposes of the agency, and good faith or legally mandated disclosure of any personal identifying information by an employee or agent of an agency for the legitimate purposes of the agency shall not constitute a breach of security.

§10-502 **Agency disclosure of a security breach** a. Any city agency that owns or leases data that includes personal identifying information and any city agency that maintains but does not own data that includes personal identifying information, shall immediately disclose to the police department any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach if such personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

b. Subsequent to compliance with the provisions set forth in subdivision a of this section, any city agency that owns or leases data that includes personal identifying information shall disclose, in accordance with the procedures set forth in subdivision d of this section, any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach to any person whose personal identifying information was, or is reasonably believed to have been, acquired by an

unauthorized person.

c. Subsequent to compliance with the provisions set forth in subdivision a of this section, any city agency that maintains but does not own data that includes personal identifying information shall disclose, in accordance with the procedures set forth in subdivision d of this section, any breach of security following discovery by a supervisor or manager, or following notification to a supervisor or manager, of such breach to the owner, lessor or licensor of the data if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

d. The disclosures required by subdivisions b and c of this section shall be made as soon as practicable by a method reasonable under the circumstances. Provided said method is not inconsistent with the legitimate needs of law enforcement or any other investigative or protective measures necessary to restore the reasonable integrity of the data system, disclosure shall be made by at least one of the following means:

1. Written notice to the individual at his or her last known address; or

2. Verbal notification to the individual by telephonic communication; or

3. Electronic notification to the individual at his or her last known e-mail address.

e. Should disclosure pursuant to paragraph one, two or three of subdivision d be impracticable or inappropriate given the circumstances of the breach and the identity of the victim, such disclosure shall be made by a mechanism of the agency's election, provided such mechanism is reasonably targeted to the individual in a manner that does not further compromise the integrity of the personal information.

§10-503 **Agency disposal of personal identifying information.** An agency that discards records containing any individual's personal identifying information shall do so in a manner intended to prevent retrieval of the information contained therein or thereon.

§3. This local law shall take effect 120 days after it shall have been enacted into law; provided that the commissioner of any agency may take any actions necessary prior to such effective date for the implementation of this local law including, but not limited to, establishing guidelines and promulgating rules.