Legislation Details (With Text)

File #:	Int 0141-2004	**Version:**	A	**Name:**	Businesses licensed by the DOA to notify consumers in the event of a security breach of personal identifying information.
Type:	Introduction			**Status:**	Enacted
				In control:	Committee on Consumer Affairs
On agenda:	2/4/2004				
Enactment date:	5/19/2005			**Enactment #:**	2005/046

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

Sponsors: Philip Reed, Gale A. Brewer, Vincent J. Gentile, Eric N. Gioia, Hiram Monserrate, Michael C. Nelson, Eva S. Moskowitz, Joseph P. Addabbo, Jr., John C. Liu, G. Oliver Koppell, David I. Weprin, Betsy Gotbaum

Indexes:

Attachments: 1. Committee Report 3/1/04, 2. Hearing Transcript 3/1/04, 3. Committee Report 3/30/05, 4. Hearing Transcript 3/30/05, 5. Opening Statement 3/30/05, 6. Committee Report 5/4/05, 7. Hearing Transcript 5/4/05, 8. Fiscal Impact Statement-A, 9. Local Law, 10. Hearing Transcript - Stated Meeting 5/11/05

Date	Ver.	Action By	Action	Result
2/4/2004	*	City Council	Introduced by Council	
2/4/2004	*	City Council	Referred to Comm by Council	
3/1/2004	*	Committee on Consumer Affairs	Hearing Held by Committee	
3/1/2004	*	Committee on Consumer Affairs	Laid Over by Committee	
3/30/2005	*	Committee on Consumer Affairs	Hearing Held by Committee	
3/30/2005	*	Committee on Consumer Affairs	Laid Over by Committee	
5/4/2005	*	Committee on Consumer Affairs	Hearing Held by Committee	
5/4/2005	*	Committee on Consumer Affairs	Amendment Proposed by Comm	
5/4/2005	*	Committee on Consumer Affairs	Amended by Committee	
5/4/2005	A	Committee on Consumer Affairs	Approved by Committee	Pass
5/11/2005	A	City Council	Approved by Council	Pass
5/11/2005	A	City Council	Sent to Mayor by Council	
5/19/2005	A	Mayor	Hearing Held by Mayor	
5/19/2005	A	Mayor	Signed Into Law by Mayor	
5/20/2005	A	City Council	Recved from Mayor by Council	

Int. No. 141-A

By Council Members Reed, Brewer, Gentile, Gioia, Monserrate, Nelson, Moskowitz, Addabbo, Liu, Koppell, 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 businesses 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 for 2002 and 2003 indicate that identity theft is 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 businesses required to be licensed by the Department of Consumer Affairs, or pursuant to provisions of state law enforced by the department, to inform individuals whenever there has been a breach of security with respect to sensitive personal information. Business people can best serve their fellow 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. Chapter 1 of title 20 of the administrative code of the city of New York is amended by adding new section 20-117, to read as follows:

§20-117. **Licensee disclosure of security breach; notification require ments**.

a. **Definitions** . For the purposes of this section,

1. 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

powered by Legistar™

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.

2. The term "breach of security" shall mean unauthorized possession 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 the licensee for the legitimate purposes of the business of the licensee shall not constitute a breach of security.

b. Any person required to be licensed pursuant to chapter two of this title, or pursuant to provisions of state law enforced by the department, that owns or leases data that includes personal identifying information and any person required to be licensed pursuant to chapter two of this title, or pursuant to provisions of state law enforced by the department, that maintains but does not own data that includes personal identifying information shall immediately disclose to the department and 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 is reasonably believed to have been acquired by an unauthorized person.

c. Subsequent to compliance with the provisions set forth in subdivision b of this section, any person required to be licensed pursuant to chapter two of this title, or pursuant to provisions of state law enforced by the department, that owns or leases data that includes personal identifying information shall disclose, in accordance with the procedures set forth in subdivision e 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.

d. Subsequent to compliance with the provisions set forth in subdivision b of this section, any person

required to be licensed pursuant to chapter two of this title, or pursuant to provisions of state law enforced by the department, that maintains but does not own data that includes personal identifying information shall disclose, in accordance with the procedures set forth in subdivision e 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.

e. The disclosures required by subdivisions c and d 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.

f. Should disclosure pursuant to paragraphs one, two or three of subdivision e 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 licensee's choosing, provided such mechanism is reasonably targeted to the individual in a manner that does not further compromise the integrity of the personal information disclosed and has been approved, or is in compliance with rules promulgated, by the Commissioner.

g. Any person required to be licensed pursuant to chapter two of this title, or pursuant to provisions of state law enforced by the department, that discards any records of an individual's personal identifying information shall do so in a manner intended to prevent retrieval of the information contained therein or thereon.

h. Any person required to be licensed pursuant to chapter two of this title, or pursuant to provisions of state law enforced by the department, who shall violate any of the provisions of this section, upon conviction

thereof, shall be punishable by a fine of not more than five hundred dollars ($500) and shall be liable for a civil penalty of one hundred dollars ($100) for each violation.

§ 3. If any section, subdivision, sentence, clause, phrase or other portion of this local law is, for any reason, declared unconstitutional or invalid in whole or in part, by any court of competent jurisdiction, such portion shall be deemed severable, and such unconstitutionality or invalidity shall not affect the validity of the remaining portions of this law, which remaining portions shall continue in full force and effect.

§ 4. This local law shall take effect 120 days after it shall have been enacted into law; provided that the Commissioner 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.

powered by Legistar™