City of Chicago

O2017-7832

Office of the City Clerk

Document Tracking Sheet

Meeting Date:	11/8/2017
Sponsor(s):	Burke (14) Hopkins (2)
Type:	Ordinance
Title:	Amendment of Municipal Code Title 4 by adding new Chapter 4-286 concerning increased protections against data breaches for Chicagoans
Committee(s) Assignment:	Committee on License and Consumer Protection

License +
Consumer
Protection

ORDINANCE

WHEREAS, the City of Chicago is a home rule unit of government pursuant to the 1970 Illinois Constitution, Article VII, Section 6(a); and

WHEREAS, pursuant to its home rule power, the City of Chicago may exercise any power and perform any function relating to its government and affairs including the power to regulate for the protection of the public health, safety, morals, and welfare; and

WHEREAS, as practically every aspect of private and public business is conducted and stored on virtual networks and warehouses, data breaches are occurring more frequently and with more potentially disastrous repercussions; and

WHEREAS, "hacks" and data breaches have a near constant strong hold on news headlines as cybercrime afflicts nations and industries throughout the globe; and

WHEREAS, for example, in 2013, the retail giant Target had its systems breached by a cyber-attack that affected more than 41 million customer payment card accounts, causing Target to pay out $18.5 million in settlement fees; and

WHEREAS, in 2014, Home Depot's systems were breached and 50 million cardholders were affected, resulting in Home Depot agreeing to pay at least $19.5 million to compensate those individuals; and

WHEREAS, Equifax is a consumer credit reporting agency that collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide; and

WHEREAS, Equifax then sells this information to third parties in the form of consumer credit reports, insurance reports, and other consumer demographic and analytics information; and

WHEREAS, on July 29, 2017 Equifax discovered evidence of a cyber security breach in their databases that stored confidential and private consumer information of approximately 143 million U.S. consumers; and

WHEREAS, consumer information compromised in the Equifax breach includes names, social security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and documents containing personal identity information; and

WHEREAS, Equifax waited 40 days to alert consumers of their private information being stolen, thereby depriving consumers of an opportunity to freeze and monitor their accounts in a timely manner and increasing the timeframe and risk of exposure; and

WHEREAS, to date, Equifax has not issued confirmation to any person that his or her information was compromised; and

WHEREAS, according to Attorney General Lisa Madigan, 5.4 million consumers in Illinois were affected by the security breach at Equifax; and

WHEREAS, to date residents of Chicago are unsure if they were affected by the data breach because Equifax has not given them individual notice; and

WHEREAS, Chicagoans have had to waste countless hours seeking information and a remedy to the data breach issue because of Equifax's negligence; and

WHEREAS, the Illinois Personal Information Protection Act provides that notice of a breach "shall be made in the most expedient time possible and without unreasonable delay" but does not specify an exact time that individuals must be given notice; and

WHEREAS, additionally, when individuals have been affected by a data breach, it is recommended they take protections by freezing their accounts; and

WHEREAS, in Illinois it costs $20 to freeze an account during a waiver, $30 to freeze it after a waiver, and $30 to temporarily freeze an account; and

WHEREAS, paying a $20-$30 fee to the company responsible for the breach is an unfair business practice, at best, individuals affected by a data breach should not have to pay for attempting to mitigate their damages; and

WHEREAS, affected individuals should receive remedies after they have been a victim of a data breach because their personal information can be used years after it is initially stolen; and

WHEREAS, Chicago has a Consumer Privacy Protection Ordinance, however, due to the increase in data breach threats, Chicagoans deserve to have increased protections against data breaches; now, therefore,

BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF CHICAGO:

SECTION 1. Title 4 of the Municipal Code of Chicago is hereby amended by adding Chapter 4-286 as follows:

4-286-010 Short title and purpose.

This ordinance shall be known as the "Chicago Data Breach Rights and Obligations Ordinance." The purpose of this chapter is to provide for the protection of consumers residing in the City of Chicago in the event a data breach occurs, compromising their private information.

4-286-020 Definitions.

As used in this Section:

(a) "Data collector" is any person or entity including but not limited to, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity or person that, for any purpose handles, collects, disseminates, or otherwise deals with nonpublic personal information for its profit, or offers the information to a third party for profit. Provided, however, that this section shall not apply to governmental agencies.

(b) "Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

(c) "Personal information" means either of the following:

(1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through breach of security:

(A) Social Security number,
(B) Driver's license number or State identification card number,
(C) Account number or credit or debit card number or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account,
(D) Medical information,
(E) Health insurance information,
(F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

(3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

4-286-030 Notice of Breach.

(a) Any data collector who conducts business in Chicago that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of Chicago whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay but shall be made no later than fifteen (15) days after the breach has been discovered, except for the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

(b) Any data collector who maintains computerized data that includes private information not owned by the data collector shall notify the owner or licensee of the information of any breach of the security system in the most expedient time possible and without unreasonable delay but shall be made no later than fifteen (15) days following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

(c) In the event that any Chicago residents are to be notified, the data collector shall notify the Business Affairs and Consumer Protection Commissioner as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected Chicago residents. The data collector shall use the contact method on file in an attempt to give notice to the affected person or business. The data collector shall make a good faith attempt to contact the individual directly to alert them of the breach.

(d) The data collector shall give public notice of the data breach in one or more newspapers of general circulation. Such public notice shall include information related to the breach and where questions may be directed.

(e) Both the public and private notice shall specify the method through which affected consumers can obtain information about the breach and specify corrective action.

(f) The data collector shall continue to update affected persons as information about the breach is received and any corrective actions are taken, until the consumer opts out or agrees that the matter has been resolved.

4-286-040 Remedies.

(a) As part of any remedy or ratification process, a company shall not require purchase or enrollment for a fee to any product or service they offer as part of their normal products for sale.

(b) As part of any remedy or ratification process, a data collector shall not require waiver of any legal recourses including, but not limited to, a right to trial or binding arbitration agreement.

(c) Nothing in this section shall be construed to limit the rights and remedies that can or shall be made available to the affected consumer.

4-286-050 Violations.

The violation of any of the foregoing Sections shall be punishable by a fine of not less than $2,000.00 nor more than $10,000.00 following Section 2-25-090 of this Code. Each day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply. Any data collector who is also a licensee who violates this section shall be subject to license and revocation proceeding as set forth in Section 4-4-280.

4-286-060 Enforcement.

This chapter shall be enforced by the Commissioner of the Department of Business Affairs and Consumer Protection who will promulgate certain rules and regulations for the enforcement thereof.

4-286-070 Severability.

If any provision, clause, sentence, paragraph, section or part of this chapter or application thereof to any person or circumstance, shall for any reason be adjudged by a court of competent jurisdiction to be unconstitutional or invalid, said judgment shall not affect, impair or invalidate the remainder of this chapter and the application of such provision to other persons or circumstances, but shall be confined in its operation to the provision, clause, sentence, paragraph, section, or part thereof already involved in the controversy in which such judgment has been rendered and to the person and circumstances affected thereby.

SECTION 2. This ordinance shall take effect thirty (30) days after passage and publication.

Edward M. Burke
Alderman, 14th Ward

Brian Hopkins 2