



Office of the City Clerk

City Hall
121 N. LaSalle St.
Room 107
Chicago, IL 60602
www.chicityclerk.com

Legislation Text

File #: R2017-830, **Version:** 1

RESOLUTION

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, Equifax also markets and sells its credit protection and identity theft monitoring services to the consumers whose personal information Equifax collects; and

WHEREAS, Congress enacted the Fair Credit Reporting Act (FRCA) to ensure fair and accurate credit reporting, to promote efficiency in the banking system, and to protect consumer privacy; and

WHEREAS, Equifax as a credit reporting agency must abide by FRCA consumers privacy protection requirements of preventing inappropriate disclosure of private information by maintaining reasonable procedures to ensure third-party disclosures are made exclusively for permissible purposes; 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, on September 7, 2017, 40 days after the breach was allegedly discovered, Equifax finally announced to the public that, due to a vulnerability in its systems, its files had been accessed by criminals for a period of time lasting at least from mid-May through July 2017; and

WHEREAS, August 2017 regulatory filings show that three Equifax executives completed stock sales totaling nearly \$2 million worth of company stock during the period in which breach information was withheld from the public; 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, it appears that Equifax willfully ignored the clear and present risk of security breaches in its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the breach; 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, as a remedy, Equifax originally offered "complimentary identity theft protection and credit monitoring" through a website they created called equifaxsecurity2017.com <<http://equifaxsecurity2017.com>>, but the service required waiver of the right to a jury trial and purported to bind users to individual arbitration; and

WHEREAS, moreover, the credit protection assistance included an automatic renewal option on the paid service after the "free" year subscription expired; and

WHEREAS, Equifax's consumer relations were called into question even earlier when, in January 2017, the Consumer Financial Protection bureau ordered Equifax and TransUnion (another credit reporting agency), to pay \$23.1 million collectively in consumer restitution and fines for deception about the usefulness and true cost of credit sold to consumers; and

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

WHEREAS, due Equifax's conduct, Chicago residents are at an increased risk of identity theft and fraud, improper disclosure of private information, and confront the need to spend added time and money to monitor their financial records; and

WHEREAS, according to the Chicago Sun Times, more than 70 class-action lawsuits have reportedly been filed against Equifax as a result of the breach; and

WHEREAS, the Massachusetts Attorney General filed suit against Equifax alleging the company knew about electronic vulnerabilities yet failed to protect consumer data; and

WHEREAS, additionally, the city of San Francisco has filed suit against Equifax claiming the company violated California state law by failing to provide timely notice of the data breach that affected Californians and failing to provide complete and clear information; and

WHEREAS, finally, Chicago has filed its lawsuit against Equifax, claiming that the breach and the manner in which it was handled violate the Municipal Code of Chicago's provisions concerning consumer fraud and deceptive business practices; and

WHEREAS, Equifax and this breach are now the subject of congressional hearings in Washington D.C.; and

WHEREAS, with what appears to be concealment of wrongdoing and effort to profiteer from it, evidence of Equifax's conduct to date offends longstanding notions of business ethics and morals; and

WHEREAS, as these legal actions and investigations begin, the Chairman and Chief Executive Officer during the activities in question, Richard Smith, is poised to retire from Equifax with a payout worth as much as \$90 million; and

WHEREAS, this City Council is called on to ensure that intrusion upon the rights of Chicagoans is not met with multi-million dollar rewards; now, therefore,

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

The Chicago City Council calls on the Equifax Board of Directors to withhold payment of any bonus, severance package, or retirement benefit from its Departing Chief Executive Officer, Richard Smith, until there is a final disposition on the matter of City of Chicago v. Equifax, Inc., filed on September 28, 2017 in the Circuit Court of Cook County and docketed as case number

Alderman, 2nd Ward

CHICAGO October 11.2017

To the President and Members of the City Council:

Your Committee on Finance having had under consideration

A resolution calling on the Equifax Board of Directors to withhold payment on any bonus, severance package, or retirement benefit from its Departing Chief Executive Officer until such time that an investigation of the 2017 breach clears Equifax from wrongdoing.

Direct Introduction

Having had the same under advisement, begs leave to report and recommend that your Honorable Body pass the proposed Resolution Transmitted Herewith.

**This recommendation was concurred in by
of members of the committee with**

(signed'

Respectfully submitted

Chairman