Arnall Golden Gregory LLP
Attorneys at Law

Daily Privacy & Consumer Regulatory Alert

Published by the Privacy and Consumer Regulatory Practice | Washington, DC Office

November 6, 2018

FEDERAL DEVELOPMENTS

Census Bureau Releases IG Report

On October 30th, the Census Bureau Inspector General's Office released a report evaluating the Bureau's risk management framework. The Risk Management Program System automates the Census Bureau's risk management framework to manage its IT cybersecurity risks. The objective of the audit was to "determine whether the risk management framework methodology adopted by the Bureau presents an accurate picture of cybersecurity risk." The audit found that the Bureau failed to follow its risk management framework process. Specifically, the report found:

- The Bureau had not continuously monitored critical security controls and failed to document the resulting risks;
- Authorizing officials lacked information about significant cybersecurity risks; and
- The Bureau did not effectively manage common controls.

STATE DEVELOPMENTS

New Orleans City Council Passes Ban the Box Ordinance

On October 18th, the New Orleans City Council passed a Ban the Box ordinance that prohibits the city and contractors from asking job applicants about their criminal history on initial job applications, which will take effect on March 1st, 2019. The city passed a similar ordinance in 2014 for classified and unclassified jobs in certain city positions, and the proposed ordinance extends this to "all entities with a city contract, grant, or cooperative endeavor agreement." New Orleans still plans to "conduct criminal background checks on all candidates and make final hiring decisions for people with records in light of other relevant information, including experience, the seriousness of any past conviction, when the incident took place and what has occurred in the applicant's life since then."

COURT CASES

OPM Data Breach Appeal

On November 2nd, the U.S. Court of Appeals for the District of Columbia heard oral arguments in an appeal over whether the federal government should provide lifetime protections for employees impacted by two data breaches disclosed by the Office of Personnel Management (OPM) in 2015. The cases were brought by the American Federation of Government Employees (AFGE) and the National Treasury Employees Union (NTEU). Plaintiffs are seeking lifetime credit monitoring and identity theft protection for affected individuals, and NTEU wants to change how OPM stores and protects personnel data. Two of the judges noted that plaintiffs incurred real costs as a result of the breach, and may face legitimate risks beyond the 10 year protections the federal government is currently offering. AFGE and NTEU also argued that OPM ignored warning signs that it was not adequately protecting data and that members have already had to deal with identity theft. The federal government argued

that the plaintiffs failed to demonstrate the relief would redress their damages. The lower court dismissed the case last year for lack of standing concluding there was no evidence the stolen information was misused.

FCRA Case

On October 11th, the U.S. District Court for the District of Columbia ruled that states are immune from lawsuits under the Fair Credit Reporting Act (FCRA) in *Pendergrass v. Washington Metropolitan Area Transit Authority (WMATA)*. Plaintiff Galen Pendergrass alleged that WMATA's criminal background check policy was discriminatory after his job offer was rescinded following a background check that found a conviction for a non-violent offense. Pendergrass claimed that WMATA's policy had a "disparate impact" on African-American candidates due to their historically higher rate of criminal convictions. The case was dismissed because the court held that WMATA's hiring policies are governmental decisions that are immune from lawsuits and decisions concerning the hiring of WMATA employees are "immune from judicial review." The court also held that neither the governments that chartered WMATA nor Congress abrogated immunity to FCRA claims.

The case is Pendergrass v. Washington Metropolitan Area Transit Authority, Civil Action No. 18-622, in the U.S. District Court for the District of Columbia.

INTERNATIONAL DEVELOPMENTS

EU Railway Announces Data Incident

EU railway service, Eurostar, sent an email informing customers to reset their passwords following unauthorized attempts to login to customer accounts, which were identified in October. Since the company does not store bank or credit card information on its systems, the only information that was potentially accessed was names and emails. Following the discovery, the unauthorized party was blocked, the UK Information Commissioner's Office was notified, and customers were instructed to reset their passwords.

This newsletter is published by AGG's Privacy and Consumer Regulatory Practice. For more information, please visit www.agg.com or contact Bob Belair, Kevin Coy, or Montserrat Miller. To subscribe, please email dpcra@agg.com.