THE WASHINGTON REPORT
May 2014

At the White House

On May 1st, the Executive Office of the President issued a report on "Big Data," entitled: "Big Data: Seizing Opportunities, Preserving Values." The Report—prepared under the direction of Counselor to the President John Podesta, Commerce Secretary Penny Pritzker and other administration officials—discusses a wide range of data issues and initiatives and makes a number of recommendations on how issues presented by "Big Data" should be addressed in areas ranging from national security to education privacy.

The Report references the Fair Credit Reporting Act (FCRA) and notes that the FCRA has limitations to its scope, it does not otherwise take a detailed look at the FCRA or tenant or employment screening.

One of the Report's primary areas of attention is the potential for the use of data to unfairly discriminate. As a result, the Report recommends that the Department of Justice, the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and the Equal Employment Opportunity Commission (EEOC), should "expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and develop a plan for investigating and resolving violations of law in such cases." It remains to be seen what steps the agencies will take to implement this recommendation.

At the FTC

"**Data Brokers**." On May 27th, the FTC issued its long awaited report on "data brokers," entitled: "Data Brokers: A call for Transparency and Accountability." While the FTC considers consumer reporting agencies to be "data brokers", the FTC Report focuses on non FCRA regulated areas including marketing, risk mitigation and people search products. While FCRA-regulated products were not the focus of the FTC Report, it nevertheless refers to the FCRA some 53 times.

The Report makes a number of recommendations that Congress consider legislation to provide for increased regulation of data brokers offering products in the marketing, risk mitigation and people search product segments. These recommendations are intended to increase transparency and enhance consumer choice. Congressional consideration of these recommendations will be important to watch because while the focus of the Report and its recommendations is on non-FCRA offerings, it is possible that any "data broker" legislation that Congress may consider could have implications for consumer reporting agencies as well.

The Report recognized that the line between an FCRA and non-FCRA product is not always a clear one. In a footnote, the FTC notes that "risk mitigation" products could be covered by the FCRA "depending upon the information collected and its use", a

point that Commissioner Brill echoed in her statement concurring in the release of the Report. The FTC will continue to look at these products on a case by case basis, noting that merely labeling an offering as a risk mitigation product does not necessarily mean that it is outside the scope of the FCRA.

The Report also reiterated the Commission's view that a disclaimer indicating that a report is not a consumer report and not to be used for FCRA permissible purposes alone is not sufficient to exclude a report from FCRA coverage if it otherwise meets the definition of a "consumer report."

Data Security. Last month's *Washington Report*, reported on developments in the FTC's ongoing data security litigation against Wyndham hotels. This month, the FTC continued to move forward in a separate data security case against LabMD, a medical testing laboratory. The LabMD case, unlike Wyndham, is proceeding before an FTC administrative law judge.

In the LabMD case, the FTC alleges that the company failed to reasonably protect the security of personal information, including medical information. The FTC alleges that in two separate breaches, the Company exposed the personal information of approximately 10,000 consumers. The complaint alleges that in one case billing information for over 9,000 consumers was found on a peer-to-peer file-sharing network and then in a separate incident LabMD documents containing sensitive personal information of at least 500 individuals were found in the possession of identity thieves.

On May 19th, the Commission denied a motion by LabMD for a summary decision in the company's favor. In doing so, the Commission rejected legal and factual arguments by LabMD that there was not a proper basis for the matter to proceed. In January, the Commission previously had denied LabMD's motion to dismiss the case a decision that a federal judge declined to overturn on May 12th in part because it was not a final agency action. LabMD has been making many of the same arguments against FTC authority to bring data security actions as Wyndham has been making in its matter, as well as arguing that the FTC should not be able to bring an action to the extent the LabMD breaches involved protected health information subject to the HIPAA privacy and data security rules.

LabMD has been vigorously defending itself in the matter and is seeking to depose Commission officials about the Commission's data security standards.

The FTC, likewise, is vigorously defending its authority to bring data security cases under Section 5. While a decision adverse to the FTC in either the LabMD or Wyndham cases could have a significant impact on FTC data security enforcement efforts under Section 5, the FTC is continuing to claim and exercise this authority under Section 5.

It is not intended to be, and should not be relied upon as legal advice. For more information, please contact Kevin Coy at 202-677-4034.