THE WASHINGTON REPORT
July 2015

On Capitol Hill

On July 23rd, Senator Brian Schatz (D-HI) introduced a bill, S. 1847, which would amend the Fair Credit Reporting Act (FCRA). This bill is co-sponsored by Senator Elizabeth Warren (D-MA) and a number of other Democratic Senators. The bill would amend FCRA sections 616 and 617 to allow private litigants to seek injunctive relief for FCRA violations and also broaden the Federal Trade Commission's (FTC) enforcement authority to include negligent and willful FCRA violations. The bill also would amend FCRA section 611 to require consumer reporting agencies to provide documentation regarding a dispute that is received from a consumer to the relevant furnisher and requiring the Consumer Financial Protection Bureau (CFPB) to gather information on consumer disputes and issue regulations regarding what constitutes reasonable procedures to ensure maximum possible accuracy under FCRA section 607(b). The bill also would require consumer reporting agencies to register with the CFPB and for the CFPB to publish registries of each type of consumer reporting agency. The bill has been referred to the Senate Banking Committee.

On July 15, Senator Sherrod Brown (D-OH) and several co-sponsors introduced a bill, S. 1773, which would amend the Bankruptcy Code to require creditors that have reported information about debts that have been discharged during bankruptcy to report, with certain limited exceptions, that the debt has been discharged and has a zero balance to any consumer reporting agency to whom they furnished that information. The bill has been referred to the Senate Judiciary Committee.

On July 13th, Representative Keith Ellison (D-MN) and several co-sponsors introduced a bill, HR 3035, which would amend FCRA section 623 to clarify that it is permissible to furnish utility and rental payment performance information, including rental payment information for units that receive subsidies from the Department of Housing and Urban Development, to consumer reporting agencies. The bill also would define the circumstances under which a utility can report payments as being late. The bill has been referred to the House Financial Services Committee.

On July 7th, the Senate Intelligence Committee reported out S. 1705, the Intelligence Authorization Act of 2016, which would require the Director of National Intelligence (DNI) to require federal agencies to implement "enhanced personnel security programs" for individuals eligible for access to classified information or eligible to hold a sensitive position. The bill would require that the enhanced personnel security program of an agency "integrate relevant information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources" as determined by the DNI. Types of information to be obtained from these sources may include: information relating to any criminal or civil legal proceeding; financial information, including credit worthiness; public information, including news articles or reports, that includes relevant security or counterintelligence information; certain publicly available electronic information including social media information; and data maintained on any terrorist or criminal watch list maintained

by any agency, State or local government, or international organization. Checks would be required at least twice every five years. The bill awaits action by the Senate.

At the Supreme Court

As the Supreme Court prepares to hear *Spokeo v. Robins* (previously reported),likely this Fall, regarding whether individuals can recover damages under the FCRA in cases where there is no concrete harm to the individual, interested parties have begun filing briefs in the case for the Court's consideration. Spokeo has filed its brief and the response brief of Robins is due next month. In the meantime, the U.S. Chamber of Commerce, the Consumer Data Industry Association, the National Association of Professional Background Screeners and numerous other parties have filed *amicus* briefs urging the court to limit the ability of plaintiffs to recover damages in cases where they have not experienced concrete harm. The Court's decision in this case could have far reaching implications for FCRA liability as well as the ability of plaintiffs to recover in a host of other privacy and consumer protection cases.

At the EEOC

On July 10th, the Equal Employment Opportunity Commission (EEOC) filed a lawsuit against Crothall Services Group, Inc. (Crothall), a nationwide provider of janitorial and facilities management services, for allegedly violating Title VII of the Civil Rights Act of 1964 by "fail[ing] to make and keep required records…that will disclose the impact that its criminal history assessments have on persons identifiable by race, sex or ethnic group." According to the EEOC's complaint, Crothall conducts criminal background checks and criminal history assessments on prospective employees and uses the information to make hiring decisions. However, according to the EEOC, Crothall does not create and maintain records indicating the impact that the background checks and assessments have in the company's hiring decisions. According to Regional Attorney Debra Lawrence of EEOC's Philadelphia District Office, "[f]ederal record-keeping requirements ensure that certain employers make and keep records that disclose the impact of their selection procedures," adding that, "EEOC's enforcement of the record-keeping requirements is important to the agency's commitment to eliminating discriminatory barriers in the workplace."

At the Office of Personnel Management

The data breach at the Office of Personnel Management continued to reverberate through Washington in July. The number of individuals potentially affected by the breach increased dramatically from approximately 4 million to over 21 million individuals, including prospective, current, and former Federal employees and contractors as well as family members, friends, and references about whom information was collected during the background check process. On July 10th, OPM Director Katherine Archeleta resigned her position as a result of the breach. The dramatic increase in the size of the breach appears to be the result of the discovery that OPM background check databases were compromised. It is not entirely clear at this point the extent to which the private firms OPM has used to assist it in the conduct of background checks played a role in the breach. The news, however, is not good for the government's background screening program, which already has been heavily criticized on Capitol Hill and elsewhere as a result of

alleged high-profile failings in connection background checks of the Washington Navy Yard shooter and Edward Snowden, as well as the termination of USIS by OPM as a result of alleged problems in the screening process.

At the FTC

On June 30, the FTC issued a guide for businesses, "Start with Security: A Guide for Businesses" highlighting lessons learned from the over 50 FTC data security enforcement actions taken to date. The ten steps discussed in the guide include:

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who's trying to get in and out.
6. Secure remote access to your network.
7. Apply sound security practices when developing new products.
8. Make sure your service providers implement reasonable security measures.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
10. Secure paper, physical media, and devices.

While the FTC promoted lessons learned from past cases, the agency also continued the administrative proceeding against LabMD over the now-defunct company's alleged data security failures. LabMD continues to vigorously resist the FTC on multiple fronts. As *The Washington Report* noted last month, the FTC denied a motion by the Company to disqualify Chairwoman Ramirez from the case. Undeterred, LabMD filed a second motion to disqualify the Chairwoman on July 15th, arguing that her communications with Congress regarding the matter have "tainted her objectivity." That motion remains pending as *The Washington Report* goes to press. LabMD also is challenging the constitutionality of the administrative proceeding itself, arguing in a motion on July 14 delegation of the authority to appoint the administrative law judge (ALJ) to OPM, is an incurable "constitutional defect." Meanwhile, the matter proceeds, with the ALJ in the case denying, on July 20th, LabMD's motion to refer Tiversa, the company that was involved in disclosure of the breach to the FTC and the source of congressional hearings over its role in the matter, to the Justice Department for a potential criminal investigation.

The FTC's data security efforts against Wyndham Hotels and others continue as well. On July 22nd, Wyndham sought to block discovery efforts while the parties engage in court-ordered mediation. The Third Circuit is still considering Wyndham's challenge to the FTC's ability to bring data security actions under section 5 of the FTC Act. Separately, on July 21st, the FTC announced that it was taking action against the identity-protection firm LifeLock for allegedly violating its obligations under the company's 2010 settlement with the FTC which requires LifeLock to implement and maintain a comprehensive information security program. Details as to the precise nature of LifeLock's alleged violations were unclear as the Washington Report went to press.

Employment and tenant screeners should consider regularly reviewing their data security program in light of ongoing guidance from the FTC and hacking incidents targeting background screening, such as the OPM breach.

.

Disclaimer: The *Washington Report* provides a general summary of recent legal and legislative developments and is for informational purposes only. 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.