SPECIAL ALERT: CFPB ENTERS INTO FIRST CONSENT ORDER WITH ONLINE PAYMENT PLATFORM FOR MISREPRESENTING DATA SECURITY PRACTICES

On March 2, the CFPB took action against an Iowa-based online payment platform and entered into a Consent Order for deceptive acts and practices relating to false representations regarding the company's data security practices in violation of 1031(a) and 1036 (a)(1) of the Consumer Financial Protection Act of 2010. The CFPB ordered the company to pay a $100,000 fine and to take certain remedial steps to improve their cybersecurity practices. Notably, this action is the result of the company's failure to have adequate controls in place; it is *not* the result of a breach incident. Similar to other regulators, the CFPB will likely pay increasing attention to cybersecurity and data privacy issues as the understanding of its significance grows.

The Consent Order states that, despite representations to the contrary, the company (i) misrepresented the quality and efficacy of its cybersecurity and data privacy practices by stating that all personal data on its site was "safe" and "secure" and that its practices "exceeded" industry standards; (ii) did not properly encrypt consumer data; and (iii) failed to provide employees with sufficient cyber training.

In addition to the fine imposed, the company must (i) adopt reasonable and appropriate data security measures to protect consumers' personal information; (ii) establish, implement, and maintain a comprehensive data security plan and appropriate data security policies and procedures; (iii) designate a qualified person to coordinate and be accountable for the data security program; (iv) conduct data security risk assessments twice annually; (v) conduct regular employee training; (vi) address required security patches to fix vulnerabilities identified in any web or mobile application; (vii) develop, implement and maintain appropriate method of customer identity authentication at registration and before effecting funds transfer; (viii) address procedures for selection and retention of service providers; and (ix) obtain an annual data security audit from an independent, qualified third party on short and specified timeframes. The Consent Order also prohibits the company from future violations of sections 1031(a) and 1036(a)(1) of the CFPA in connection with marketing, advertising, and promotion or administration of its electronic payment networks.

The Board is required to review all plans, reports, programs, policies and procedures required by the Consent Order prior to submission to the CFPB and authorize any necessary actions for the company to fully comply with the Consent Order. The Board will have ultimate responsibility for "proper and sound management" of the company and for ensuring that it complies with Federal consumer financial law and the Consent Order.

The Consent Order also contains various reporting, recordkeeping and compliance monitoring requirements. Finally, the Consent Order does not bar the CFPB, or any other governmental agency, from taking additional action against the company.

* * *

Questions regarding the matters discussed in this Alert may be directed to any of the persons listed below, or to any other BuckleySandler attorney with whom you have consulted in the past.

- Andrew L. Sandler, (202) 349-8001
- Douglas F. Gansler, (202) 349-8058
- Elizabeth E. McGinn, (202) 349-8050
- Margo H. Tank, (202) 349-8050
- James T. Shreve, (202) 461-2994
- Dana V. Syracuse, (212) 600-2326
- Rena Mears, (202) 349-7977