CFPB TO FINANCIAL COMPANIES: BEEF-UP DATA PROTECTION MEASURES OR FACE REGULATORS' WRATH

Ana M. Cabassa-Torres

The Consumer Financial Protection Bureau ("CFPB") recently released the Consumer Financial Protection Circular 2022-04 ("Circular") warning that financial companies, including non-bank financial firms like fintech companies and credit reporting agencies, may be liable for failing to adequately protect consumer data. According to the Circular, the failure to implement and maintain adequate security practices to protect sensitive personal information could "constitute an unfair practice" under the Consumer Financial Protection Act ("CFPA"). With this Circular, it is clear that the CFPB will increase scrutiny and enforcement over companies that mishandle consumer data.

Key Aspects of the CFPB's Data Security Circular

As an initial matter, the Circular states that an actual data breach is not a prerequisite for an organization to violate the CFPA's prohibition on unfair practices.

The Circular describes conduct that may typically meet the first two elements of an unfairness claim – (i) likely to cause substantial injury to consumers and (ii) not reasonably avoidable by consumers. The Circular explains that if companies fail to implement "reasonable cost-efficient measures to protect consumer data," they might be more likely to trigger liability for unfair practice under the CFPA. The CFPB defines "reasonable cost -efficient measures" to include the following:

1. Implementing multi-factor authentication ("MFA") for employees and offering it to consumers as an option to access the systems and accounts.

2. Adopting password management policies and practices, including processes to prevent employees from re-using passwords compromised in breaches at other companies.

3. Engaging in timely and routine software updates and patches to deal with security vulnerabilities within programs or products.

All companies should take active measures to reduce the risk of mishandling consumer data, including revisiting their policies and procedures, oversight processes, and training.

How Redgrave LLP Can Help

Redgrave LLP can help navigate this changing regulatory environment. Our team's unique blend of legal and technical knowledge and skills can assist your organization with developing policies and procedures to protect personal data stored in your organization's

systems. We can advise organizations to take active measures to safeguard personal data, including the following:

- *Classify the data and assess all risks and threats to the data.* Companies should develop data classification policies and perform a risk assessment to identify various threat actors and risks to the data, including cyber risks and physical security vulnerabilities.

- *Maintain and test key access controls, including complex and unique passwords and MFA.* Companies should revise their policies to require employees and users to use credentials unique to the organization. Companies should also use network zoning and related techniques to separate sensitive systems handling financial data from other systems and manage access controls on a need-to-know and role-based basis.

- *Software updates and patch management.* Companies should implement policies and procedures to ensure that their organization keeps software current with the most recent patch version. Many companies subscribe to threat intelligence for a list of industry threats and trends, emerging cyber vulnerabilities, and available patches and fixes to strengthen systems and prevent breaches.

- *Perform a gap assessment against the GLBA Safeguards Rule and other applicable laws.* Although the Circular states that compliance with GLBA Safeguards Rule is not a safe harbor against liability under the CFPA, the requirements of the GLBA Safeguards Rule can serve as a helpful baseline for compliance with the CFPA. Those requirements range from administrative requirements to appoint a head of your information security program and to conduct documented risk assessments to technical requirements on adopting encryption, access controls, and multi-factor authentication.

- *Encryption and backup are critical.* Hackers are deleting backups found on compromised systems. Therefore, organizations need to have data backups encrypted with a copy stored offline.

- *Conduct security training.* As human error is often the root cause of a cyber vulnerability, companies are increasing the frequency and scope of security training. Companies often test their staff's preparedness to detect and avoid various phishing techniques and scams employed by hackers to gain access to the organization's systems.

- *Data minimization.* Companies should perform routine defensible disposition to dispose of data and information companies no longer need for a business, legal, or regulatory reason. Reducing the amount of consumer data and personal information a company maintains helps reduce the risk and impact of a data breach.

For assistance with or additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.