Breaking Down the FTC's Hard-Press Against CafePress: Five Takeaways from the Recent FTC Action

April 29th, 2022 | and K. Dailey Wilson

The Federal Trade Commission ("FTC") recently took action against CafePress, an online customized merchandise platform, for violations stemming from its data security practices. *See In re Residual Pumpkin Entity, LLC* (d/b/a CafePress). Specifically, the FTC alleged that CafePress:

- Stored Social Security numbers and other information in clear, readable text;
- Retained sensitive customer data longer than necessary;
- Failed to encrypt passwords and answers to password reset questions;
- Failed to engage in monitoring and testing of its data security measures; and
- Failed to adequately respond to a security incident, taking seven months to notify government entities and affected consumers of the incident.

The FTC asserted that CafePress's data security failures constitute an unfair act or practice – consumers allegedly likely suffered an actual injury because breached personal information is often used to commit fraud and identity theft; that CafePress's alleged failure to adequately respond to the security breach led to an unreasonable delay in consumer notification of the data breach, increasing the likelihood that the consumers would become victims of fraud and identity theft; and consumers allegedly could not have reasonably avoided harms posed by CafePress's failures because they had no way of independently knowing of the data breach.

Among other things, the proposed settlement requires the company to pay $500,000 in redress, to provide notice to consumers about the security breach and settlement with the FTC, to develop and maintain an information security program, and to submit to third-party security assessments, the results of which must be provided for public disclosure.

Several insights can be gleaned from the complaint and order in the *CafePress* action, but we're going to focus on just a few.

The expectation to secure data extends beyond financial institutions. It is clear that the FTC expects all entities maintaining sensitive customer information to develop and maintain effective data security measures. The federal Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. The CafePress action shows that the FTC can and will use its UDAP authority to effectively require non-financial institutions (including, for example, rent-to-own providers,

retailers, and medical services providers) to develop and maintain an information security program that is commensurate with that required under the Safeguards Rule. In fact, the FTC ordered CafePress to establish, implement, and maintain an information security program that essentially mirrors that outlined in the newly-revised Safeguards Rule, requiring encryption of certain information, penetration and vulnerability testing, addition of data access controls, and implementation of multi-factor authentication.

Don't ignore security incident claims. Companies maintaining customer information should not ignore reports of potential security incidents. The timeline associated with CafePress's security incident, as alleged by the FTC, shows an alleged failure to appropriately respond to the incident:

- March 11, 2019: received first notice of its February 2019 security incident.
- March 12, 2019: internally confirmed existence of system vulnerability.
- April 10, 2019: received email notification from foreign government informing CafePress of security incident.
- April 15, 2019: required users to reset passwords due to updates to its password policy.
- July 13, 2019 to August 5, 2019: publication of internet posts by third parties exposing security incident.
- September 2019: sent breach notification letters and emails to government agencies and affected consumers and posted notice of breach on the CafePress website.

The FTC's complaint alleges that CafePress failed to notify consumers of a potential security incident for seven months, despite receiving multiple notifications from third parties that a security incident had occurred. Notably, although breach notification generally is an issue of state laws (which the FTC does not enforce), the FTC cited to CafePress's alleged failure to notify consumers as part of its claim that the actions of the company constituted an unfair act or practice because it allegedly hampered the ability of consumers to protect themselves from harm. Companies should take any notification of a potential security incident seriously and immediately investigate and respond to such incidents in accordance with the company's written incident response plan, including assessing notice to consumers.

Develop and implement a disposal policy. Companies should retain sensitive customer information only for as long as necessary for business operations or as otherwise required by law or regulation. The FTC alleged that CafePress indefinitely stored sensitive customer information on its networks without regard to whether there was a legitimate business need for such information, ultimately creating unnecessary risk. Companies should implement and maintain a disposal policy that addresses how long customer information is maintained and how that information is securely disposed of once there is no legitimate business or legal reason for retaining the information.

FTC will still seek consumer redress in UDAP cases post-*AMG*. For decades, relying on Section 13(b) of the FTC Act, the FTC regularly ran straight to federal court with UDAP claims allegedly violative of Section 5 and sought court-ordered monetary relief. Last year, the Supreme Court's *AMG v. FTC* decision unanimously rejected that decades-long practice and explained that Section 19's administrative process is the congressionally prescribed path to monetary relief for Section 5 claims. Following *AMG*, some practitioners have questioned the FTC's basis for obtaining monetary relief at all in settlements in UDAP cases. Through their affirmative votes

in *CafePress*, along with other Section 5 cases settled post-*AMG*, the Commissioners have made clear their bipartisan agreement that the FTC may obtain the same relief in settlement that it could eventually, maybe, get under Section 19 at trial, including money. They differ, however, on their interpretations of the types of monetary relief permitted under Section 19. In their dissenting statement issued in *In re Resident Home LLC*, for instance, the Republican commissioners asserted that Section 19's authorization of relief "necessary to redress injury to consumers" limited the Commission to restitutionary relief, that is, relief designed to make consumers whole and not to be a penalty or disgorgement. Because they found the monetary award proposed in *Resident Home* to exceed any reasonable estimate of actual consumer injury, they viewed the settlement as exceeding Section 19's grant of authority. The Democratic commissioners, in contrast, found the Republican's reading of the statute to be too restrictive, contending that Section 19 permits "damages," including consequential damages to both consumers and businesses, and besides that the statute contemplates relief not explicitly enumerated ("Such relief may include, but shall not be limited to …"). In any case, said the Democratic commissioners, in settlement the FTC is not bound by the type of relief it could have been awarded at trial. The takeaway here being, while the Commission's makeup remains as it is now, split two-two along party lines, we can expect any monetary relief included in an order settling strictly UDAP claims to be based on a restitution theory, or else it would seem unlikely to receive the necessary votes. Of course, the confirmation of a fifth (Democratic) Commission will change this calculation.

Expect consumer notice order provisions only in privacy and data security cases – for now. As part of its proposed settlement with the FTC, CafePress would be required to provide notice to consumers to inform them of the breach incident as well as details of the settlement. Such requirements are not too controversial or uncommon, but they were also not necessarily a given in every privacy or data security case. Take *In re LightYear Dealer Technologies, LLC* for example, an FTC action from 2019 alleging that an auto dealer software provider failed to take reasonable steps to protect consumers' data, leading to a breach that exposed personal information about millions of consumers. The facts were not all that different from those in *CafePress*, yet the settled order required no notice to consumers.

More recently, the Democrats on the Commission have been pushing for the FTC to presumptively seek notice provisions in privacy and data security matters, especially in matters that do not include consumer redress. In fact, consumer notice requirements have been appearing more regularly in settlements, including, but not limited to, privacy and data security cases. *See, e.g.*, Order, *In re Lithionics Battery, LLC* (misrepresenting products in violation of the Made in USA Labeling Rule); Order, *In re Support King, LLC* (stalkerware app sharing user location and other data). For their part, Republican commissioners have signaled opposition to such a presumption, preferring an assessment of the appropriateness of consumer notice on a case-by-case basis. In his separate statement issued in *In re Flo Health, Inc.*, for instance, Commissioner Noah J. Phillips argued that consumer notice has historically been used in cases only where there is a need to inform consumers about some ongoing harm or can take some remedial action. And so, while the Commission remains evenly bipartisan, the Phillips view on consumer notice provisions might, to some degree, cabin notions of seeking such notice in orders as a matter of course.