UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA

Regarding Ascension Data & Analytics
Commission File No. 1923126
December 14, 2020

Summary

- After an egregious data breach involving extremely sensitive financial information, the Commission has struck a settlement that provides no help for victims and does little to deter.
- It appears Ascension Data & Analytics is really just an offshoot of a large investment fund, and the Commission's proposed order fails to bind the appropriate parties.
- To achieve meaningful results, the Commission must reevaluate its enforcement strategy when it comes to safeguarding consumer financial information by working collaboratively with other regulators and applying its unfairness authority in an even-handed manner.

Americans have been burned by the mortgage industry before – not just by slipshod practices that maximize profits at the expense of responsible stewardship, but also by slippery accountability when things go wrong. Regulators got lost in a labyrinth of shell companies and subsidiaries, and too many who profited escaped unscathed, leaving families in ruin.

To achieve the dream of homeownership, Americans typically have to fork over a boatload of personal data to mortgage lenders, like our Social Security numbers, our driver's license numbers, our pay stubs, and more. This is the norm when you borrow to buy a home. The lender then transfers this data onward through the financial system, with banks, servicers, mortgage funds, investment vehicles – and their vendors – all gaining access.

This data, in the wrong hands, is valuable intelligence not only for identity thieves but also for nation states, leading to threats to our financial and national security. That's why federal law ensures that financial institutions have safeguards in place to secure this highly sensitive data.

After a data breach of highly sensitive data from mortgage applications, the FTC launched an investigation into Ascension Data & Analytics. Ascension worked on behalf of its sister companies, such as investment funds to analyze mortgages. Ascension also hired other vendors to help. Even though Ascension was required under the law to guard consumer financial data, in fact, they were using third parties with shoddy security, as alleged in the complaint. Given the breadth and sensitivity of the data compromised in this breach, an individual consumer would probably prefer to be affected by the Equifax breach than this one, if forced to make a choice.

In my view, the Commission's proposed resolution of this investigation suffers from three key flaws: It fails to hold all of the right parties accountable. It fails to charge unfair conduct as unfair. And it fails to redress consumers or deter other firms from engaging in similar misconduct.

Ascension, Rocktop Partners, and Corporate Musical Chairs

Ascension is not really an independent company.[1] It's in the same corporate family as Rocktop Partners,[2] a multi-billion dollar private equity fund that buys up defective mortgages, such as those with title disputes.[3] Ascension's President, Brett Benson, is also Managing Director of Rocktop Partners.[4] Its office sits on the same floor as Rocktop Partners at 701 Highlander Boulevard in Arlington, Texas.[5] When the Ascension breach hit the news, it was Rocktop's General Counsel, Sandy Campbell, who confirmed the key details of the incident.[6] It is unclear whether Ascension has any clients *other* than Rocktop Partners or others in its corporate family.[7] This is a common arrangement in finance, since it allows fund managers to profit when they can bill their investors for services.

Further, Rocktop's Managing Director and Chief Financial Officer, Jonathan Bray, is also the sole person ("manager" or "member") listed on the LLC forms for a firm called Reidpin LLC.[8] Langhorne Reid and Jason Pinson ("**Reid**" and "**Pin**son") are cofounders of Rocktop.[9] Unsurprisingly, Reidpin LLC is located at the same address as Ascension and Rocktop.[10] It is therefore clear that Ascension is anything but arms-length from Rocktop. Rocktop's corporate structure confirms this conclusion:

Figure 1. [redacted]

The FTC has charged Ascension Data & Analytics – but not any other parties in the broader Rocktop family – with violating the Safeguards Rule by failing to police its agents processing personal data. I

[1] My office has endeavored to cite public sources showing a portion of the web of companies involving Ascension, Rocktop, and Reidpin LLC.
[2] Zack Whittaker, *Millions of bank loan and mortgage documents have leaked online*, TECHCRUNCH (Jan. 23, 2019), https://techcrunch.com/2019/01/23/financial-files/.
[3] ROCKTOP PARTNERS, https://rocktoppartners.com/ (last visited on Oct. 2, 2020).
[4] *Id.*
[5] *Id.*, Compl., *In the Matter of Ascension Data & Analytics, LLC*, Fed. Trade Comm'n File No. 1923126.
[6] *Supra* note 2.
[7] *Id.*
[8] Reidpin, LLC, Application to Register a Foreign Limited Liability Company (LLC) (Nov. 17, 2020) https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=201816410221-24379676.
[9] *Supra* note 3.
[10] *Supra* note 8.

agree that Ascension violated the law, but I am concerned that the proposed settlement will do little to prevent future failures. In addition, our complaint and the Analysis to Aid Public Comment would be strengthened with critical information about the Rocktop corporate structure.[11]

The FTC's order binds only one company: Ascension. The company that actually appears to manage more than $7 billion worth of Americans' mortgages – Rocktop – is not being required to change a single thing about its practices.[12] And while Ascension will be required to clean up its act, nothing is stopping the controllers of Rocktop from creating a "new" analytics firm staffed with exactly the same executives, or even transferring the functions within their corporate family, but without any obligations under the FTC's order. This would be economically rational. The Commission does not cite any sworn testimony or other evidence to show why they believe the controllers of Ascension would act irrationally.

Commissioner Phillips argues that this is a concern in cases involving "boiler rooms and other frauds." I respectfully disagree. When the FTC charged Wyndham in 2012 with lax data security practice, it named not only the parent corporation but also three subsidiaries, alleging that they operated with common control, shared offices, overlapping staff, and as part of a maze of interrelated companies. Defending these charges against dismissal, the Commission argued that "[i]f the Court were to enter an order against only [the subsidiary], Wyndham would be able to transfer responsibility for data security to another Wyndham entity[,]" allowing the company to sidestep its obligations under any order.[13] The court agreed, specifically rejecting the view that only "shell companies designed to perpetrate fraud" can face charges.[14]

The FTC should not be allowing companies to evade accountability through a game of corporate musical chairs. An effective order would bind not only Ascension, but also all of the parties liable under the law. While one of these parties may be outside the jurisdiction of the FTC's Safeguards Rule, there is no question that they are bound by the FTC Act's prohibition on unfair practices.

Unfair Conduct is Unlawful, Regardless of Size

The FTC has declined to include a charge of violating the FTC's prohibition on unfair practices. This represents a departure from previous cases involving similar misconduct, and raises questions as to whether the FTC is engaging in disparate treatment based on business size and type, rather than on facts and evidence.

In 2014, the FTC charged Ajay Prasad, Shreekant Srivastava, and their company, GMR Transcription Services, with violating the FTC Act's prohibition on unfair practices when it failed to ensure its vendors protected sensitive data. As detailed in the Commission's complaint, GMR failed to ensure that their vendors implemented reasonable security measures, and failed to prevent one vendor from storing sensitive files in plain text. The complaint does not allege that malicious actors attacked the vendor's systems, nor does it allege that GMR's failure to oversee the vendor directly led to the

[11] Commissioner Phillips points to the fact that Rocktop Partners may be a registered investment fund under the securities laws, but does not discuss the other entities within the corporate family and in any related mortgage vehicles that are not.
[12] *Supra* note 3.
[13] *Fed. Trade Comm'n v. Wyndham et al.*, 2013 WL 11116791 (D.N.J. May 20, 2013).
[14] *Fed. Trade Comm'n. v. Wyndham Worldwide Corp.*, 2014 WL 2812049, at *7 (D.N.J. June 23, 2014).

improper data disclosure, but nevertheless charges both the firm and its owners with engaging in unfair business practices by failing to employ reasonable security measures.[15]

If GMR faced this scrutiny, why wouldn't Ascension? The FTC's complaint alleged that GMR's lax policies created a vulnerability that was exploited at least once, and the FTC's complaint in this matter details some of the consequences of this catastrophic breach, which involved dozens of actors, mainly from overseas, including those with IP addresses in China and Russia. They were able to access more than 60,000 Americans' sensitive financial information. Furthermore, in failing to prevent this mass theft, Ascension disregarded its own risk management policies, failing to take "any of the steps described in its own policy to evaluate [its vendors'] security practices."[16]

Taken together, the allegations against Ascension leave little doubt that the company's practices were unfair, causing far more unavoidable injury than GMR, without any apparent benefit to consumers or competition.[17] When the Commission settled with GMR, the law was exactly the same. The only thing that changed is the five members of the Commission.

My colleague suggests there are questions about whether Ascension's practices were unfair, but the Commission's complaint details how elementary the missteps were that led to this breach. A reasonable person would expect if these problems could have been prevented simply by Ascension following its own vendor management policies. Ascension could have also heeded the FTC's 2015 business guidance, which warns firms to "[m]ake sure service providers implement reasonable security measures."[18]

My colleague also cites instances where the Commission has charged a firm with violating the FTC's Safeguards Rule without also including charges of unfair practices. However, these cases do not involve conduct related to inadequate service provider oversight, which is the core allegation at issue with Rocktop and Ascension.

We must apply more evenhanded enforcement to ensure that large businesses and investment firms are not getting less scrutiny than small businesses. The Commission's failure to charge Ascension and its affiliates with an unfairness violation is not only inconsistent with prior practice but also undermines our ability to hold the company accountable for its failures.

Rethinking Remedies

The most effective way to address serious data breaches like this one is to compensate the victims, penalize the wrongdoers, and insist on changes to the responsible company's practices. Unfortunately, the Commission's proposed order misses the mark on identifying the responsible company, while doing nothing to compensate victims or penalize those responsible for this

[15] Compl., *In the Matter of GMR Transcription Services, Inc.*, Fed. Trade Comm'n File No. 1223095 (Aug. 21, 2014), https://www ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.
[16] Compl., *In the Matter of Ascension Data & Analytics, LLC*, Fed. Trade Comm'n File No. 1923126.
[17] *See* 15 U.S.C. § 45n Defining as unfair practices that cause or are likely to cause substantial injury that is not reasonably avoidable, and is not outweighed by benefits to consumers or competition.
[18] START WITH SECURITY, A GUIDE FOR BUSINESS, LESSONS LEARNED FROM FTC CASES, FED. TRADE COMM'N (Jun. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

catastrophic breach. I am therefore not confident that the remedies proposed in today's order will deter other companies from engaging in the same slipshod practices.

We could have done more. I recognize that consumers harm can be difficult to estimate in these cases, and that the Commission lacks civil penalty authority for offenses like this one. But that problem can be solved. The FTC is not the only enforcer in this space – dozens of state attorneys general and financial regulators can enforce a nearly identical unfairness authority under federal law that is backed up with strong tools to both seek redress and penalties. By partnering with a state enforcer, the Commission can dramatically improve its data security actions – ensuring that there is compensation for victims and consequences for wrongdoing.[19]

Unfortunately, the FTC almost never invites state regulators, particularly state banking regulators with significant expertise, to join our investigations and enforcement actions to obtain additional relief when it comes to data protection. This must change.

Conclusion

We should all be unconvinced that chasing after dangerous data breaches and resolving them without any redress or penalties is an effective strategy. Making matters worse, holding a "company" accountable that is really just an extension of a financial firm might allow our order to be completely ignored. After this settlement, Ascension could "fold," and the Rocktop family of companies can reconstitute it, escaping any obligations under the order.[20]

The FTC is currently considering changes to its rule on safeguarding consumer financial information.[21] But, we also need to rethink our enforcement strategy. Our go-it-alone strategy is doing nothing for breach victims and little to deter, and our two-track approach to unfairness is penalizing small companies while giving a pass to financial firms like Rocktop. For these reasons, I respectfully dissent.

---

[19] In addition to having unfairness jurisdiction, many state enforcers have their own versions of the Safeguards Rule. *See, e.g., Industry Guidance Re: Standards for Safeguarding Customer Information and Regulation 173*, NEW YORK STATE DEP'T OF FIN. SERV., https://www.dfs ny.gov/insurance/ogco2002/rg204021.htm.

[20] For context, public information indicates that there are seven companies with interrelated officers or agents currently active, including "Reidpin LLC," "Reidpin, LLC," "Reidpin Investments, LLC," Reidpin Rocktop 1, LLC," "Reidpin Rocktop III, LLC," "Reidpin Rocktop IV, LLC," "Reidpin Rocktop V, LLC" founded in 2011, 2014, 2015, 2016, two in 2017, and one in 2018. There are two other entities with these characteristics which appear to have folded. https://opencorporates.com/companies?q=REIDPIN%2C+LLC.

[21] Fed. Trade Comm'n., Standards on Safeguarding Customer Information, 84 Fed. Reg. 13158 (Apr. 4, 2019), https://www federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information.