

# Explainer Things: Episode 8

August 31, 2023



It's been the summer of the pop star—with nonstop news of Taylor Swift and Beyonce selling out stadium after stadium. Don't let it “break your soul” as you're “shaking off” summer and sending the kids back to school. We hope at least some of them will be joining the diving team and practicing the triple lindy in a nod to the late, great Rodney Dangerfield and the 80s classic *Back to School*.

In the meantime, you can continue to expect blurbs relevant to payments, crypto, fintech, cards, and more, with our quick analysis (aka Akerman's Take) on why that news matters to you. If you have suggestions or questions about the newsletter, email us at [explainerthings@akerman.com](mailto:explainerthings@akerman.com).

---

## Related Work

Consumer Financial Services, Data and Technology (CFS+)

---

## Related People

- [William P. Heller](#)
- [Tyler B. Engar](#)
- [Eric I. Goldberg](#)
- [Christy S. Hawkins](#)
- [Thomas J. Kearney](#)
- [Aliza Pescovitz Matouf](#)
- [Nora Rigby](#)
- [Chelsea D.B. Valente](#)

---

## Subscribe to Explainer Things

[Click here](#) to receive future editions and stay on top of developments in consumer finance law.



- [A...B...R? Always Be Refinancing: CFPB Sues Installment Lender for Steering Customers to Refinance](#)
  - [No More \*Mr. Robot\*: New SEC Rules Aim to Prevent Hacking](#)
  - [CFPB Rule on Data Brokers: “Why Do I Feel Like, Somebody’s Watching Me?”](#)
  - [FedNow Payments System: Catch Me If You Can?](#)
  - [TCPA Update: Stop Calling, Stop Calling, I Don’t Wanna Talk Anymore](#)
  - [Once, Twice, Three Times a... Privacy Framework?](#)
- 

[Episode 7](#)

[Episode 6](#)

[Episode 5](#)

[Episode 4](#)

[Episode 3](#)

[Episode 2](#)

[Episode 1](#)

## A...B...R? Always Be Refinancing: CFPB Sues Installment Lender for Steering Customers to Refinance

---

The CFPB filed a [three-count UDAAP action](#) against a non-bank installment lender alleging it essentially forced customers to refinance past due loans. According to the complaint, Heights Finance Holding Co. made most of its profit from borrowers who refinanced their loans rather than paying them off. The complaint’s extensive statement of facts cites internal emails, training materials, and compensation policies focused on encouraging refinancing. For example, one directive stated, “When a customer has paid the loan down to just a few payments, they start focusing on paying us out. We can combat that by refinancing them now!” Among the practices listed, the lender did not allow partial payments and refused to extend due dates. It

also labeled refinance offerings as “fresh starts” even though they carried the same term as the original loan and required payment of new origination fees. As a result of repeated refinancings, borrowers received less cash back from each refinancing, as more of the loan went to pay fees and interest on prior loans.

There are three separate UDAAP claims. The first alleges unfairness and finds that harm is not reasonably avoidable for three reasons—because borrowers are (a) “financially vulnerable,” (b) the lender does not accept partial payments, modify terms, or extend due dates, and (c) borrowers cannot afford to make payments to get current on their loans. In the second, CFPB asserts abusive conduct because the lender took advantage of the borrowers’ lack of understanding of the risks of refinancing. For the third, CFPB charges abuse, again, because the borrowers cannot protect their own interests in selecting a loan because they have no other options.

This is only a complaint; the lender has yet to respond to the allegations.

## Akerman's TAKE

Remember when Alec Baldwin acted in dramatic feature films, instead of TV comedies? Way back in 1992, he played the lead in the Oscar-winning movie *Glengarry Glen Ross*, giving the world the classic sales advice “Always be Closing.” Maybe the tag line for Heights Financing is “Always be Refinancing”? Other lenders should probably not follow that motto since CFPB believes pushing people to refinance is unfair and abusive.

Whether that theory will prevail is unclear, though. While heavy on factual allegations, some of the bases for alleging unfairness and abusiveness appear legally underwhelming. We imagine that the lender will raise these issues in defending itself. That said, CFPB has always focused on short-term lenders who “trap”

consumers in a cycle of debt. Lenders with similar business models should be wary.

From a big picture angle, this lawsuit may indicate CFPB is concerned its Small Dollar Lending Rule will not take effect soon or will not stem certain harmful practices if it does take effect. The future of the Small Dollar Lending Rule (and the entire CFPB) is pending before the Supreme Court this fall. Even if CFPB wins, the Small Dollar Rule contains only some of provisions from the original 2017 rule, because the agency removed the rule's mandatory underwriting provisions under its prior Republican director. This lawsuit may be a sign of CFPB's move away from rulemaking and towards effecting change through quicker methods, such as enforcement.

## No More *Mr. Robot*: New SEC Rules Aim to Prevent Hacking

---

SEC announced its new rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies. Under the new rules, a registrant must disclose a cybersecurity incident to SEC within four days after determining an incident is material. The disclosure needs to include the material aspects of the nature, scope, and timing of the incident, as well as likely impact on the registrant. This means that as part of your investigation into a cybersecurity incident, you need to make sure you get answers for these specific areas as quickly as possible.

The regulation requires a registrant to describe its processes for assessing, identifying, and managing material cyber risks and their likely effects. This means they expect you to have them and be able to

demonstrate compliance. The regulation also requires registrants to describe the board of directors' oversight of cybersecurity risks. While they are important, the items included here just scratch the surface of the 180+ pages that make up the new rules, which generally take effect for annual reports on fiscal years ending on or after this December.

## Akerman's TAKE

*Mr. Robot's* main character Elliott was a cybersecurity engineer by day and a hacker by night. SEC's new rules aim to make Elliott's hacking side-hustle more difficult, but would likely make his day job harder in the short run, too. The rules leave quite a bit for publicly traded companies to unpack. While guidance is given in the form of specific requirements in the rules, how each company implements them will depend on their operations and what is practical for the company in complying with the rules. One thing that companies should not overlook is the value gained by updating their incident-response plans. By building the disclosure topics and assigning them to an incident-response team member, companies can reduce the risk of these things being de-prioritized and can include the deadline to ensure timely reporting. A robust but flexible incident-response plan can serve as evidence of working processes for assessing, identifying, and managing material cyber risks and their likely effects. In addition to reflecting board oversight of cybersecurity risks in meeting minutes, a company may wish to update its incident-response plan to define the criteria that will trigger notification to the board and assign an incident-response team member the responsibility of communicating with it.

# CFPB Rule on Data Brokers: “Why Do I Feel Like Somebody’s Watching Me?”

CFPB Director Rohit Chopra announced an upcoming rulemaking aimed at prohibiting “harmful data broker practices.” He made the announcement at a White House roundtable on the risks associated with artificial intelligence. The rule is intended for companies harvesting data from multiple sources, then monetizing individual data points or profiles, sometimes by sharing the data with the companies that use AI to make predictions and decisions. According to Chopra, the rule will propose to cover these data brokers as “consumer reporting agencies” under the Fair Credit Reporting Act (FCRA). That would mean that data brokers would be required to adhere to certain standards regarding accuracy of information and how the information is used, as well as permit consumers to access the information about them and dispute errors in that information. Additionally, the proposal would clarify whether “credit header data” is a consumer report covered by the FCRA. Credit header data includes identifiers like name, date of birth, and social security numbers and is not currently considered a “consumer report” covered by FCRA. Director Chopra said the agency plans to release an “outline of proposals” in September, which is a required step CFPB must take before issuing a notice of proposed rulemaking.

## Akerman's TAKE

We all know very little about us remains private in our increasingly digital world. It’s something people have been worried about for a long time, even as far back as 1984 with Rockwell’s only hit, “Somebody’s Watching Me.” Director Chopra could be a fan of 80s music, but even if not, there’s a lot to unpack in this rulemaking announcement. This appears to be the

mysterious FCRA rulemaking announced on this spring's Unified Agenda, which stated only that the agency would be amending the regulations that implement the FCRA—nothing about how or why. It sounds as if the proposed rule would significantly expand the meaning of the term “consumer reporting agency” to include data brokers who are not currently covered by the statute. If enacted, this would give consumers significantly more power over their data in the murky world of personal data sales—allowing them to challenge errors and know exactly what information is in their data file.

We expect the “newly covered” data brokers to fight hard against the proposal, including on the grounds that CFPB does not have the statutory authority to expand FCRA’s definition of “consumer reporting agency.” Of note, this would be the agency’s first discretionary FCRA rulemaking in its 12-year history. It amended the rules that implement FCRA once in 2022 to address a Congressional mandate on human trafficking and otherwise has made only technical changes to the rules.

## FedNow Payments System: Catch Me If You Can?

---

At the end of July, the Federal Reserve launched its instant payment infrastructure “FedNow,” available all day, every day. FedNow is marketed as a complement to ACH services, which take between one to three business days to settle payments. To facilitate these faster transfers and anticipated volume, FedNow has integrated “Dropp,” powered by Hedera’s hashgraph consensus network, to make smaller transactions more feasible. Dropp is a pay-by-bank alternative to credit card payments which

allows merchants to accept small-value purchases digitally at a lower cost than credit cards.

Financial institutions are expected to eventually adopt FedNow in order to offer faster services for customers, including account-to-account transfer, request for payment, bill pay, etc. The Federal Reserve is encouraging more than 9,000 financial institutions to sign up for FedNow, providing the following options to interested financial institutions: (1) send and receive; (2) receive only; (3) liquidity management transfers; and (4) settlement services.

## Akerman's TAKE

The Federal Reserve is seemingly making it easier for banks (especially smaller ones) to join the digital age, using blockchain technology to hasten transaction speeds. Touting itself as a safe and efficient way to transfer funds instantly, it will be interesting to see in these first few months if any bugs or hackers cause the service to be interrupted. One imagines there are budding young criminals out there who have seen *Catch Me If You Can* and would love to find a way to run scams on the network (and maybe get played by Leo DiCaprio in a movie!). The government has been very focused on addressing anti-money laundering issues in recent years, but the Fed has not said much on how FedNow will implement the laws aimed at preventing money laundering.

Financial institutions and their customers may want to consider a few things: First, while FedNow may be charging low fees now, it is likely that the service will increase fees later. How much? Who knows? FedNow has the potential to affect private financial interests, including current services like Zelle and the revenue from processing credit card transaction fees. There also may be the possibility that the current grace periods customers enjoy for mortgage payments, student loans, and other



debts will shrink as processing times for payments speed up.

## TCPA Update: Stop Calling, Stop Calling, I Don't Wanna Talk Anymore

---



Lots to report this month in TCPA news, below are some of the highlights.

- Twelve Democratic senators, including Senators Markey, Lujan, Warren, and Klobuchar sent a letter to the FCC on August 7 asking it to align itself with recent guidance issued by FTC, with respect to telemarketing calls. In particular, the senators are seeking to (1) have FCC limit the scope of consumer consent to only agreements between the seller and the consumer (i.e. no lead generators) and (2) restrict consent to only an agreement between a *single* seller and a consumer. The senators argue FCC does not need to issue new regulations to institute these changes because the regulations from 2003 and 2012 already provide FCC with necessary authority.
- The Florida Telephone Solicitation Act is more viable than previously thought. FTSA contains anti-spoofing restrictions designed to prevent callers from using fake numbers to call consumers. In particular, “telephonic sales calls” must come from numbers a consumer can call back and speak to a telephone solicitor. A “telephonic sales call” includes text messages, but many of the numbers used to send marketing text messages are either short codes or phone numbers that are not set up to receive call backs. As a result, enterprising plaintiffs’ attorneys are testing a new FTSA theory and claiming marketing text messages violate these anti-spoofing requirements. They are asserting the

new notice and cure provisions added to FTSA earlier this year do not bar these lawsuits because those requirements do not apply to the anti-spoofing restrictions. This is a novel theory, and we are likely to see a number of these lawsuits filed before courts issue any guidance.

- On August 8, 2023, the Ninth Circuit confirmed text messages are not, in fact, prerecorded voice messages under TCPA. The court looked to the ordinary meaning of the word “voice” and concluded that to qualify as a prerecorded voice there must be “an audible component.” It’s unclear from this decision, however, whether a text message that sends a video or contains an audible sound would qualify as a prerecorded voice under TCPA.

## Akerman's TAKE

After a brief dip following the Supreme Court's decision in *Facebook, Inc. v. Duguid*, it seems TCPA world is heating up again. And it looks like there are some big changes ahead for callers engaging in telemarketing. Now more than ever, compliance with state and federal telemarketing laws is essential. If you aren't ready to follow Lady Gaga's advice and just “Stop Calling,” you might want to double check your TCPA compliance in light of these recent developments.

## Once, Twice, Three Times a... Privacy Framework?

---


The U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration have developed and agreed on the new Data Privacy Framework (DPF) Program to allow personal data that is subject to European Privacy Laws (such as Europe's General

Data Protection Regulation (GDPR) and the corresponding UK GDPR) to be lawfully transferred to the U.S. Many companies are proceeding with caution, if at all, in certifying under the DPF after learning Austrian activist Max Schrems has committed to challenging the decision. Schrems previously challenged and defeated two predecessor privacy frameworks. Certification involves a thorough analysis of a company's data privacy practices and protections and ultimately a commitment by a company to implement and maintain certain data practices. The idea is that, after a company has certified, they will no longer undertake more burdensome methods to assure others they can receive and process personal data in compliance with applicable laws. For companies considering certifying (or re-certifying) under the new DPF Program, there are three important considerations.

First, the DPF requires a certifying company to choose an independent recourse mechanism that will be available to investigate unresolved complaints. A company can choose to (1) cooperate with EU, Swiss, and UK data protection authorities or (2) use a different independent recourse mechanism.

Second, there are core principles that each have specific requirements. These principles include: (1) notice, (2) choice, (3) accountability for onward transfer, (4) security, (5) data integrity and purpose limitation, (6) access, and (7) recourse, enforcement, and liability.

Third, similar to the GDPR, companies must be able to verify their compliance with the DPF principles—mere compliance isn't enough.

Akerman's TAKE 

Like the lady who captured Lionel Richie's heart,

not just once or twice, but three times (a lady) maybe the third time is the charm for this European privacy framework? Because of the impending challenge to DPF, it's difficult to tell whether the juice (new privacy compliance measures) will be worth the squeeze (making international data transfers less complicated). The troubled history of the Safe Harbor, Privacy Shield and now DPF may make some organizations wary of allowing personal data transfers to the U.S. solely based on DPF. We've seen this film before—companies who invested substantial time and resources into Privacy Shield were forced to sink more into privacy compliance and international data transfer mechanisms after Privacy Shield was invalidated. If you're considering certification, we're here to help, especially with the three considerations noted above. Investing resources in things like privacy technology to assist with privacy requests, enhanced security measures, and creating documentation to demonstrate compliance won't be all for naught, even while we wait to see whether there will be widespread certification under DPF. Time will tell. In the meantime, we can all watch for the "we've updated our privacy policy" notices.

---

Explainer Things is brought to you by the Consumer Financial Services, Data & Technology Practice Group (CFS+) at Akerman LLP.

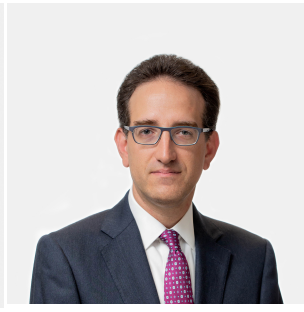
For questions about the items in this issue, please contact us at [explainerthings@akerman.com](mailto:explainerthings@akerman.com).

**- EXPLAINER THINGS CAST -**

---



**Bill Heller**



**Eric Goldberg**



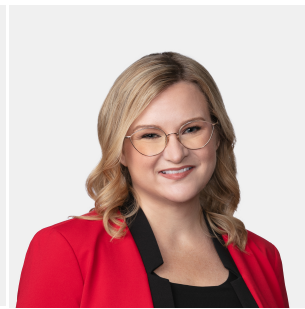
**Tom Kearney**



**Tyler Engar**



**Nora Rigby**



**Christy Hawkins**



**Aliza Pescovitz Malouf**    **Chelsea D.B. Valente**

---

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.