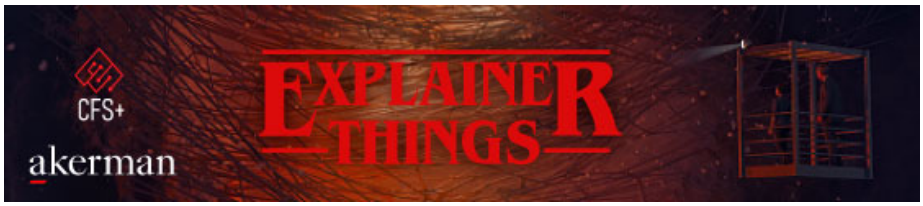
akerman

Practice Update

Explainer Things: Episode 4

April 28, 2023



This season of Explainer Things is progressing nicely, don't you think? We've introduced our recurring characters, like cryptocurrency, data privacy, and CFPB Director Rohit Chopra. We've established the tone – lighthearted but informative. Read to the end of this episode for our fresh perspectives on payments, fintech, cards, and more, with our quick analyses (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 .

IN THIS ISSUE - EPISODE 4

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
- Nora Rigby

Subscribe to Explainer Things

Click here to receive future editions and stay on top of developments in consumer finance law.

Previous Episodes

Episode 3

- Are Peer-to-Peer Payment Apps Systemically Risky Business?
- Data Makes a Comeback in the CFPB's Small Business Lending Rule
- So the SEC Just Won't Let Crypto Be
- Influencers Beware, the FTC Might Be One of Your Followers
- States Tackle Minors' Social Media Usage
- The Rodeo Continues: U.S. State Privacy Law Roundup

Episode 2

Episode 1

Triple Threat: CFPB Releases Policy Statement on Abusiveness

In the entertainment world, a triple threat is someone who can sing, dance, and act. The CFPB's version of the triple threat is its ability to prevent unfair, deceptive, *and* abusive practices. There is a significant body of law built up around the meaning of unfair and deceptive, but much less about what constitutes an abusive practice. The CFPB wants to change that and recently issued a policy statement outlining its view of what makes conduct abusive. We couldn't wait for this episode of *Explainer Things* to write about this policy statement, so please read our recent client alert from earlier here.

Are Peer-to-Peer Payment Apps Systemically Risky

Business?

CFPB Director Rohit Chopra is continuing to focus on the risks posed by large non-bank providers of consumer financial services. In recent remarks, he indicated the Financial Stability Oversight Council (FSOC) (on which he sits) should consider deeming large-scale payments platforms as "SIFIs," or systemically important financial institutions. Since 2010 there have been four designations (none of them payments platforms) and all have since been rescinded. In his remarks, Director Chopra focused on fraud risks to consumers as well as the safety and security of customer funds. Previously, the CFPB has expressed concern about whether Regulation E and other laws adequately protect consumers from certain types of fraud it believes is too common on these platforms. Additionally, Director Chopra indicated he is concerned customer funds on these platforms are not protected by FDIC insurance, unless held at an insured institution. If the FSOC deems these companies SIFIs, regulators will be allowed enhanced oversight. Perhaps not coincidentally, earlier this month the FSOC proposed changes to its rules that would make it easier to designate nonbanks as SIFIs. That could mean the FSOC is already heading in the direction that Director Chopra suggests for some payments platforms.

Akerman TAKES

It appears Director Chopra reached conclusions about the systemic risk of peer-to-peer platforms even without completing the CFPB's study of big tech companies it announced (with much fanfare) in 2021. Director Chopra also appears focused on what the FSOC might do as opposed to examining whether rules implemented by the CFPB—namely Regulation E's Prepaid Accounts and Remittance Rules—adequately protect

consumers from the risks posed by these platforms. It's possible Director Chopra is concerned he lacks the authority to extend Regulation E to reach the fraud that occurs on these platforms. As for security of customer funds, the Prepaid Rule—which applies to mobile wallets that store consumers' funds—requires that providers disclose whether consumers' funds are FDIC insured. We can expect the CFPB to evaluate the effectiveness of this disclosure in its forthcoming assessment of the Prepaid Accounts Rule.

Data Makes a Comeback in the CFPB's Small Business Lending Rule

After many years in development, the CFPB finalized its small business lending rule (also known as the "1071" rule for the section of the Dodd-Frank Act that directed the CFPB to issue it). Despite its name, the rule does not impose any requirements on small businesses. Instead, it requires financial institutions that offer credit to small businesses to report data about the applications they receive and the loans they make. Similar to the data that lenders must report on home mortgages, this rule is intended to make it easier to enforce fair lending laws with respect to small business lending.

The rule requires data submissions from many different types of lenders, including banks, credit unions, online lenders, platform lenders, nonprofit lenders, and merchant cash-advance providers. Whether a lender is required to report data to the CFPB depends on if the businesses it lends to are small (generally under $5 million in annual revenue) and the number of loans it makes to those businesses. Lenders who make fewer than 100 loans

annually to small businesses are not required to report data to the CFPB. Lenders who make more than 100 loans annually are required to begin reporting data on different schedules, starting with the largest lenders who make more than 2,500 small business loans annually. Those lenders must begin collecting data in October of this year and reporting it by summer of 2024. Lenders that originate fewer small business loans have longer to begin collecting and reporting the data. The CFPB provides compliance guides for lenders who must begin reporting data on its website.

Akerman TAKES

Data is really having a moment. First, Ke Huy Quan returned from career obscurity to win the Oscar for Best Supporting Actor (you know, Data from the Goonies). Then, the CFPB finalizes the first fair lending data-collection rule since Regulation B implemented HMDA in the 1970s. The CFPB took nearly 13 years to finish this rule and might never have done so had it not been sued; likely because a data-collection rule is hardly a quick win – it will take years for consumers to feel the benefits of this rule whereas lenders *and consumers* will start to feel the costs immediately. Smaller credit unions are already saying they may reduce their small business lending because it's simply not worth the cost and hassle. Only time will tell. The bottom line: If you lend money to small businesses, take a look at this rule now because, sooner or later, you'll be collecting and reporting data.

So the SEC Just Won't Let Crypto Be

Although April was not as litigious as March for SEC crypto enforcement, the agency still reported two lawsuits against crypto companies and executives. In one, the agency sued beaxy.com and its executives for allegedly failing to register as a securities exchange, broker and clearing agency. The agency also charged Beaxy's founder, Artak Hamazaspvan, with raising an unregistered offering ($8M), of which he purportedly misappropriated $900K. In the other case, the SEC charged crypto trading platform Bittrex, Inc., and its former CEO William Shihara also with failing to register as a securities exchange, broker and clearing agency. The lawsuits are similar and reflect the SEC's continued insistence that crypto exchanges, in particular, register as securities exchanges, brokers or clearing houses.

Interestingly, during his April 18 testimony before the House Financial Services Committee, SEC Chair Gary Gensler appeared unable to provide a clear or coherent answer to a question about why crypto is a security rather than a commodity. At the same time, he rebuffed Republican criticisms the SEC is ill-equipped to regulate crypto and driving crypto companies from the U.S. with its regulation-by-enforcement approach (well, at least until companies comply with existing regulations). And, as if intentionally coordinated, while Mr. Gensler was giving testimony, Federal Reserve Governor Michelle Bowman made it clear she believes the harm of a U.S. central bank digital currency would outweigh the benefits.

Akerman TAKES

Much like the FCC to Eminem in the early aughts, the SEC just won't let crypto be. Are folks right to be concerned the SEC and other regulators' policies will drive crypto companies to foreign countries? Yeah, we think so, and, apparently, so does Coinbase CEO Brian Armstrong. During a meeting earlier this month with UK politicians, Mr. Armstrong sang their

praises for moving fast on crypto regulation, while begrudging the Wells notice the SEC issued Coinbase back here in the US. All the while Hong Kong banks continue their push to draw crypto companies to the Asian markets, including a unit of China's state-owned Bank of Communications.

Assuming U.S. regulators would prefer not to spur investment in foreign markets, why not direct attention and resources to innovation and updating regulations instead of reaffirming a commitment to regulation-by-enforcement? The SEC should take a cue from the NYDFS, who clearly believes crypto isn't a flash in the pan; it adopted its first virtual-currency regulation nearly eight years ago. This month, the NYDFS announced it adopted a regulation giving it authority to collect supervisory costs from licensed virtual currency businesses (like it does to other licensees) to continue investing in top talent, tools, and other resources to provide effective oversight. You know, treating crypto regulation like the regulation of other financial products and assets. While the NYDFS system is not without its challenges, it is at least an attempt to create clear rules of the road.

We get it, crypto is a square peg. And what do we do with square pegs? Well, we don't sue them just for being square pegs. Rather, we do like the Apollo 13 ground crew did when the Co2 filters on the lunar module proved inadequate. We put our minds and resources to the task and "invent a way to fit a square peg in a round hole ." Like astronauts need clean, breathable air, the financial industry, including crypto companies, needs regulatory clarity to survive. And bringing it full circle, "sorry [Mr. Gensler], your [agency's crypto] problem's complicated."

Influencers Beware, the FTC Might Be One of Your Followers

The FTC recently sent penalty notices for offenses concerning substantiation of product claims and product endorsement or testimonials in advertisements to over 700 companies. In the notices , the FTC reminds advertisers they cannot "make an objective product claim without having a reasonable basis...consisting of competent and reliable evidence." The notices state advertisers must be clear about the relationship between the company and the endorser, including disclosing any material connections between the two that consumers may not otherwise expect. The notices go on to state it is an unfair or deceptive trade practice for advertisers to falsely claim a product is endorsed by a third party or imply the endorser is an actual, current, or recent user of a product when they are not. Finally, the notices remind advertisers they cannot "use a testimonial to make unsubstantiated or otherwise deceptive performance claims, even if such testimonials are genuine" but should instead use testimonials which represent a user's typical or ordinary experience with the product. Any of the 700 companies who received these notices and later violate them could be subject to a civil penalty of up to $50,120 per violation.

Akerman TAKES

Influencers are everywhere these days, amirite? It seems just about every major brand incorporates statements from one influencer or another to promote its products. From beer (we're not going here), to crypto (B-list celebs still count, right?), to cheeseburgers (oldie, but still a goodie). The FTC stated in May 2022 it was going to be updating its endorsement guidelines to "crack down on fake reviews and

other forms of misleading marketing." The 700 notices make us think the FTC was serious; preventing deceptive advertising remains a top priority – who needs updated enforcement guidelines, anyway? Companies take heed! Evaluate your advertising claims to ensure they have adequate support. And while we all might find testimonials to be compelling, let's make sure the experience depicted actually represents an average user's experience.

States Tackle Minors' Social Media Usage

In the preceding months, states have increased focus on minors' usage of social media. In March, Utah passed Senate Bill 152 to regulate how minors interact with certain social media platforms. Once the law is effective, social media companies must:

- Verify the adult age of a Utah resident seeking to maintain or open a social media account;
- Get the consent of a parent or guardian for users under age 18;
- Allow parents full access to their child's account;
- Create a default curfew setting that blocks access overnight (10:30 pm to 6:00 am), which can be adjusted by parents;
- Prohibit direct messaging by anyone who the child hasn't followed or friended; and
- Block underage accounts from search results.

In addition, social media companies won't be permitted to collect children's data (beyond what is required to verify their age and maintain their account) or target their accounts for advertising.

Violations of the Utah bill come with hefty fines: $250,000 for using addictive design features, and up

to $2,500 per child exposed to an addictive feature. Parents will also be able to sue social media companies directly for certain harms.

Arkansas also passed a bill on children's social media, which will ban minors under 18 from most social media platforms without parental consent. Like the Utah law, Arkansas Senate Bill 396 also requires social media platforms to verify users' ages.

Akerman TAKES

For both the Utah and Arkansas laws, it is unclear exactly how they will be enforced, and critics have expressed other concerns with practicality and first amendment violations, among other things. Keep an eye out for lawsuits challenging these laws in the coming months, because, as Shoeless Joe Jackson taught, "if you [ban] it, they will come." In addition, look for other states to follow suit in passing similar laws – Texas, Ohio, Louisiana, and New Jersey are already on their way. And other states, such as Montana, are looking to ban entire social media networks.

The Rodeo Continues: U.S. State Privacy Law Roundup

Congrats to Indiana, Montana, and Tennessee, the three newest states to join the comprehensive privacy law club. In all likelihood, Indiana will become the seventh (or eighth, depending on Montana and Tennessee) state to pass a comprehensive privacy law, current Senate Bill 5, assuming Governor Eric Holcomb doesn't veto it. Indiana's bill is similar to the laws in Connecticut, Colorado, Virginia, Utah, and Iowa in addressing a

business's obligations to provide a privacy notice, allowing for consumers to exercise their rights in their personal data, and imposing contract requirements for any vendors handling personal data. If passed, the new Indiana law would become effective on January 1, 2026.

The Montana legislation, Senate Bill 384 , unanimously passed and is headed for the governor's signature, and if passed would take force on October 1, 2024. Tennessee SB 73 is also awaiting enactment pending the governor's signature, and if passed, it would take effect on July 1, 2025.

Akerman TAKES

Indiana's bill is very similar to the law passed in Virginia, which may give Indiana companies and others who do business there at least some sense of practical application. Montana's bill is a bit of a hodge-podge, and Tennessee takes some significant steps that we haven't seen in any privacy law to date – it requires companies to adhere to the NIST privacy framework. Businesses facing the onslaught of new U.S. privacy laws are taking each state law as they come – inconsistencies, contradictions, and all – which, in reality, may make privacy transparency and choices more difficult for consumers. As we've said before, one of the most practical ways to digest the forthcoming privacy laws is to take a holistic approach to identify common denominators, what currently is and will be required, and what makes the most sense for the business to prioritize to prepare for what's coming. That's, again, our approach to the Indiana, Montana, and Tennessee likely-to-be laws.

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.

EXPLAINER THINGS CAST

Bill Heller

Eric Goldberg

Tom Kearney

Tyler Engar

Nora Rigby

Christy Hawkins