

Explainer Things: Season 2 Episode 3

June 5, 2024



It has been a busy time for us at *Explainer Things*. Awards season is over, but the fintech regulatory drama is in midseason form. The star of this episode is of course the Supreme Court’s decision on the future of the CFPB. The case ushered in a bunch of spinoffs in terms of two CFPB actions—an enforcement action against Solo Funds and an interpretive rule applicable to Buy Now Pay later—that appear to have been waiting in the wings. In other news, the longest running show in ET history—privacy legislation—continues rolling on. See below for the latest updates there. Finally, we have a wrap up to the legislative season with several new earned wage access laws to digest and a potential summer blockbuster rulemaking from California. And, as we went to press, the CFPB continued to issue new rules and guidance on “deception in contract fine print,” treatment of wire transfers under Regulation E, and a purported “registry to

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 Malouf](#)
- [Nora Rigby](#)

Subscribe to Explainer Things

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



detect corporate repeat offenders.” We’ll cover that and more in future episodes. You can continue expecting 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.

Previous Episodes

[Season 2, Episode 2](#)

[Season 2, Episode 1](#)

[Episode 11](#)

[Episode 10](#)

[Episode 9](#)

[Episode 8](#)

[Episode 7](#)

[Episode 6](#)

[Episode 5](#)

[Episode 4](#)

[Episode 3](#)

[Episode 2](#)

[Episode 1](#)

- IN THIS ISSUE - SEASON 2, EPISODE 3 -

- [It’s “No Time to Die” for the CFPB as Supreme Court Holds Agency Is Constitutional](#)
 - [In New BNPL Guidance, the CFPB Says a Browser Extension Has Always Been a Credit Card](#)
 - [New CFPB Complaint Alleges Fintech Loan Marketplace Violated Consumer Financial Protection Act and FCRA](#)
 - [California \(Maybe\) Says Earned Wage Access Is a Loan? “No,” say South Carolina and Kansas; “Maybe” says Wisconsin](#)
 - [Synapse’s Bankruptcy: An “Unhappy” Surprise for Fintechs and BaaS](#)
 - [Too Much of a Good Thing? American Privacy Rights Act Advances to Full Committee](#)
 - [U.S. Privacy Law Round-Up: The Rodeo Is a State of Mind](#)
-

It’s “No Time to Die” for the CFPB as Supreme Court Holds Agency Is Constitutional



Last month, the Supreme Court decided the latest constitutional issue related to CFPB. This is the third such issue the Court has decided in the agency’s relatively brief history. For the first time, the Court sided with the agency, finding the CFPB’s funding does not violate the Constitution’s Appropriations clause. The Court upheld the structure that insulates the CFPB from Congressional appropriations and funds the agency through the Federal Reserve System’s earnings. The majority opinion was written by Justice Clarence Thomas who was joined by 6 other justices, including conservative Justices John Roberts, Brett Kavanaugh, and Amy Coney Barrett. Only Justices Samuel Alito and Neil Gorsuch dissented.

Immediately after, the CFPB, following a victory lap, indicated it will set new effective dates for its Small Business Lending Rule:

Compliance Tier	Original Compliance Date	New Compliance Date	First Filing Deadline
Tier 1 institutions (highest volume lenders)	October 1, 2024	July 18, 2025	June 1, 2026
Tier 2 institutions (moderate volume lenders)	April 1, 2025	January 16, 2026	June 1, 2027
Tier 3 institutions (smallest volume lenders)	January 1, 2026	October 18, 2026	June 1, 2027

This likely resolves the outstanding challenge to the small dollar lending (payday loan rule). Upon remand, we expect the court to lift the stay and new compliance dates to be set for that rule, as well.

Akerman's TAKE

Your Explainer Things cast is on pins and needles waiting for the new James Bond actor to be announced after Daniel Craig hung up his martini shaker following 2021's *No Time to Die*. Much like James Bond has for the past 60+ years, the CFPB has managed to escape death over and over again since its creation in 2010. Perhaps the agency's director will start introducing himself as "Chopra, Rohit Chopra." In any event, most of the pundits who follow the Supreme Court predicted this outcome ever since oral arguments last October, during which several justices expressed skepticism about the novel constitutional theory raised by the plaintiffs. Director Chopra and the many people employed by the CFPB must be breathing easier this week knowing their jobs are secure for now (as are the pensions of former CFPB employees here at ET).

We predict this will be the end of constitutional challenges to the mere existence of the CFPB and future agency litigation will focus on the merits of the cases, rather than on the agency itself. We also predict this decision will open the floodgates for more CFPB enforcement actions because lower courts will no longer put such cases on hold pending the outcome of the latest constitutional challenge. In the short time since the decision, the CFPB has filed two new enforcement actions. The decision, coupled with the CFPB's recent hiring spree in the Office of Enforcement, means that consumer finance companies should pay close attention to compliance for the foreseeable future.

In New BNPL Guidance, the CFPB Says a Browser Extension Has Always Been a Credit Card

In one of its first post-Supreme Court regulatory actions, the CFPB issued a short “interpretive” rule subjecting BNPL providers to some of the credit card rules in Regulation Z. Some being the operative word—they never actually say which ones (that’s, we guess, where we come in). By issuing an interpretive rule, the CFPB is announcing a new interpretation of Regulation Z without revising it or its commentary. The CFPB asserts that consumers’ digital accounts that they can repeatedly use to obtain a BNPL loan are the same as credit cards, because both are devices that can be used from time to time to obtain credit.

While subpart B of Regulation Z is titled “open-end credit,” and credit cards typically access open-end credit, some (but not all) of the credit card provisions of subpart B apply to card issuers that extend “credit that is not subject to a finance charge and is not payable by written agreement in more than four installments.” Some of Regulation Z’s provisions are likely now applicable to BNPL card issuers including rules related to the investigation of disputes and billing errors, rules around refunds, and a requirement to provide certain account opening disclosures and periodic statements.

Provisions in subpart B that only apply to open-end credit would not apply to BNPL, nor would most of subpart G, as the CARD Act largely applies only to open-end credit. The CFPB also explains that the rule applies to business-purpose BNPL loans when accessed by a digital user account.

Most concerning, CFPB allowed providers only until July 30 to comply with this new guidance. That's before the August 1 comment deadline. As noted, compliance is no easy task. For example, the CFPB previously estimated it takes existing card issuers 174,000 burden hours to provide periodic statements to credit card customers. Additionally, the CFPB does not commit to responding to comments on any schedule, or at all.

Akerman's TAKE

Like a long-awaited blockbuster that fizzles when it finally premieres, this guidance is a disappointing result of two years of CFPB analysis. It also doesn't follow the rules of the genre. Previously, when extending old rules to new products (*e.g.*, CFPB's 2017 prepaid account rule and the Federal Reserve's 2006 payroll card rule), the CFPB used a legislative rulemaking (notice and comment) process to explain in detail how the old rule applies to the new project after soliciting and responding to public comment. Not only did CFPB skip that step here, but it also provided no guidance on how a BNPL provider is actually supposed to comply with rules designed for open-end credit. Compliance here, in the timing given, may prove challenging.

New CFPB Complaint Alleges Fintech Loan Marketplace Violated Consumer Financial Protection Act and FCRA



The CFPB filed a complaint against SoLo Funds, Inc., a fintech company operating a peer-to-peer marketplace for short-term, small-dollar loans. The

lengthy complaint alleges SoLo engaged in advertising, originations, and servicing practices that violated the Consumer Financial Protection Act and the Fair Credit Reporting Act.

According to the CFPB, SoLo gathered credit information about applicant's bank accounts, card usage, and prior Solo loans, created a "SoLo score," and provided the score to potential lenders. The CFPB alleges that by preparing and providing this score, SoLo acted as a consumer reporting agency under FCRA. The CFPB further alleges that SoLo then violated FCRA by failing to take steps to ensure the maximum possible accuracy of the SoLo score. The complaint includes a separate FCRA claim regarding SoLo's alleged attempts to coerce payment by falsely threatening to report borrowers to credit bureaus.

The complaint also alleges SoLo asks applicants to pay tips to lenders and donation fees to SoLo. The CFPB claims that these tips and donations are finance charges because the tips or donations are paid on virtually all loans originated. CFPB alleges TILA disclosure and advertising violations.

The CFPB additionally claims SoLo "deceptively, unfairly, and abusively" serviced some loans because the loans were either made by an unlicensed person or were made in excess of state usury limitations. The complaint includes a list of state laws that SoLo purportedly violated, which the CFPB claims render many loans void or uncollectable and justify UDAAP claims against SoLo.

Akerman's TAKE

The CFPB has followed actions by state regulators in Connecticut and the District of Columbia. It's not every day you see CFPB alleging violations of Alabama, Arizona,

Connecticut, Idaho, Illinois, Indiana, Maryland, Massachusetts, Minnesota, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, and Oregon law. Many enforcement actions include alleged UDAAPs and the CFPB has increased its focus on FCRA violations. Like throwing mud against the wall, it will be interesting to see which of these numerous complaints sticks. It's also the first time since the CFPB's Small Dollar Lending Rule in 2017 that the CFPB has addressed the payment of tips and whether those payments could be finance charges. As some EWA lenders follow this approach, this may be a sign of the CFPB's approach to tip-based programs.

California (Maybe) Says Earned Wage Access Is a Loan? "No," say South Carolina and Kansas; "Maybe" says Wisconsin

In early May, the California DFPI posted on its website its long-awaited "final" regulations on earned wage access and income share agreements. We use quotes, because late last month the California Office of Administrative Law publicly rejected these rules for various technical reasons. While the DFPI will have to fix these issues and resubmit the rule for approval, we don't expect their substance to change (although DFPI may solicit an additional round of comments on the fixes).

Under the soon-to-be-final text, DFPI deems many existing EWA programs (termed "income-based advance programs" by the DFPI) to be loans under California law. However, if these providers register with the DFPI, they would be exempt from the fee restrictions/rate caps that apply to traditional

lenders in California under the California Financing Law.

DFPI also provided its Statement of Reasons addressing the many comments it received during the process. With respect to its initial proposal to impose rate caps, DFPI acknowledges its failure to conduct a proper economic impact analysis. As a result, DFPI decided to withdraw the rate cap portion of the proposal.

While this is going on, the legislative sessions wrapped up in several states. Through those processes, we saw new EWA laws passed in South Carolina, Kansas, and Wisconsin. These states adopted similar laws to those previously adopted in Nevada and Missouri. South Carolina and Kansas made clear that EWA is not a loan; Wisconsin did not address this question. EWA providers must register with each state and comply with certain consumer protections designed to distinguish EWA from traditional loan products.

Akerman's **TAKE**

The debate in the states continues to grind on. While lending laws may vary by state, the issues with EWA are the same—will regulators and legislatures continue to allow consumers to access lower-cost liquidity products or will they shoehorn these products into an ill-fitting loan structure? We here at ET have long been on the record that the latter is better. Treating these as unique products subject to oversight ensures consumer protections while allowing consumers alternatives to traditional, higher cost options.

Synapse's Bankruptcy: An "Unhappy" Surprise

for Fintechs and BaaS

You may have seen Synapse Financial Technologies in the news lately. Synapse is (or was) a Banking as a Service (BaaS) platform company. Meaning, it provided a platform that offered fintechs and other nonbanks access to business and consumer banking products (e.g., loans, credit cards, prepaid cards, bank accounts, etc.) with Synapse's banking partners. Synapse was one of the most mature of the platform companies—founded in 2014—which, in part, is why its demise is so newsworthy.

On April 22, Synapse made headlines by filing a Chapter 11 bankruptcy petition, but the demise story clearly didn't start there. Synapse's troubles began no later than September 2023, when a Synapse banking partner, Evolve Bank & Trust, notified Synapse it would be ending their partnership and seized \$16 million. In a private letter response to Evolve, Synapse CEO Sankaet Pathak raised concerns about bank charges, underpayments, rebate revenue withholding, and reconciliation challenges, ultimately intending to collaborate and resolve issues raised, but to no avail. On the heels of Evolve's decision to part ways with Synapse, one of Synapse's largest customers, Mercury, announced it would not be renewing its contract, leading Synapse lay off 40 percent of its workforce in October 2023 (after laying off 18 percent a few months before). Things continued to devolve for Synapse over the following months to the point it was looking for a buyer. Enter TabaPay, who on April 19, offered to purchase Synapse's assets for \$9.7 million in a deal requiring bankruptcy court approval. But, on May 9, TabaPay pulled out of the purchase citing a “failure to meet the purchase agreement closing conditions.”

Following TabaPay's reversal, the Synapse bankruptcy devolved into a bit of a horror show, with thousands of consumer and business accounts frozen at Evolve and other banks that held funds for Synapse customers. While the bankruptcy judge has

done an impressive job of managing the actual case—addressing significant funds-access issues and recently appointing a Chapter 11 trustee—the parties’ infighting and finger pointing is nothing short of a disaster. Thank goodness Mr. Pathak is able to file documents with the bankruptcy court from his accommodations in Santorini, Greece (see [here](#)).

Akerman's **TAKE**

Commentary among the parties to the Synapse bankruptcy—being read by platform businesses that can’t make payroll or consumers with frozen funds—are dismaying. Like, “Hey, look, we’re sorry we’re doing this to you. It’s really not intentional. We’re just doing what we have to. And, besides, it’s not our fault. So, good luck!” That finger-pointing reminds us of the *Happy Gilmore* scene when Happy arrives at Grandma’s house to find an IRS agent inventorying and assessing the home for a tax sale. The agent tells Happy, “I’m not taking her stuff, ok, the government is ... Don’t get mad at me ... I have no discretion here, her stuff is now our stuff.” Sure, we get it, it’s the other guy’s fault that businesses and consumers cannot access their funds.

While the parties’ finger-pointing and distancing don’t make the problem go away, they do highlight a grave issue for businesses operating in the BaaS space: Are you prepared for similar breakup? Will your clients and customers be faced with difficulties accessing their funds? What happens if/when you must wind down a product or a partnership? What is the potential fallout and how will it affect your business and your customers? Are these scenarios properly addressed in your program agreements? What does it mean to be properly addressed? These are some of the more important questions you should be asking when entering into a new BaaS relationship or evaluating your existing

programs so you're not caught off guard in the event of a failure.

While we all like a good surprise, like learning about the *Happy Gilmore* sequel, bad surprises are the worst. Don't be caught unprepared.

Too Much of a Good Thing? American Privacy Rights Act Advances to Full Committee

In April 2024, Senator Maria Cantwell and Representative Cathy Rodgers released a bipartisan proposal for a new federal privacy law, known as the American Privacy Rights Act (APRA). APRA builds off of an earlier proposal that failed last year. As it currently stands, APRA is slated to advance to full committee review but its viability as legislation is to be determined.

APRA is an enormous piece of legislation, but here are a few key points:

- “Covered entit[ies]” subject to APRA include: (1) entities subject to the Federal Trade Commission Act; (2) common carriers subject to Title II of the Communications Act of 1934; or (3) nonprofit entities. “Covered data” under APRA is similar in scope to the definition of personal data in existing state privacy laws. Among those exempt from APRA are government entities, entities acting on behalf of government entities, individuals not acting in a commercial context, and nonprofit organization whose primary purpose is to prevent fraud. Small businesses are also exempt, so long as the business has an annual gross revenue not exceeding the “size standard in millions of dollars specified in” 13 C.F.R. §121.201, did not collect

“covered data” for more than 200,000 individuals, and did not sell “covered data.”

- APRA would preempt any state laws, rules, regulations, requirements, prohibitions, standards, or any other provision covered by APRA, but it contains a laundry list of exemptions that wouldn’t be preempted. Most notably, APRA includes carve-outs for California and Illinois residents bringing civil lawsuits, and allowing them to recover the same relief available under either the California Consumer Privacy Act or Illinois’ Biometric Information Privacy Act or Genetic Information Privacy Act.
- APRA’s data collection limitations and prohibitions are similar to those under many state privacy laws and generally limit data collection to only data necessary, proportionate, and limited to provide or maintain a specific product, service, or non-marketing communication.
- Under APRA, consumers would have similar rights to what is currently provided by state privacy laws, including the rights to access, correct, delete, and export “covered data.”
- APRA also expands the situations where consent is required for certain data processing activities, with “Affirmative Express Consent” being required in certain circumstances, including to
 - Transfer sensitive “covered data” to a third party
 - Collect, process, retain, or transfer biometric or genetic information
 - Collect, process, retain, or transfer “covered data” to measure and analyze the market or market trends
 - Participate in a “bona fide loyalty program”
 - Retain “covered data” after it is required to be deleted by law or is no longer needed

Despite ongoing debate, APRA currently establishes a private right of action and does not allow for

mandatory arbitration clauses where the claim involves a minor, damages over \$10,000, or allegations of physical or mental harm.

Akerman's TAKE

APRA covers a lot of ground which, in theory, could make compliance easier, especially since it preempts many states' privacy laws. But sometimes too much of a good thing can be a bad thing, particularly where, due to external pressures, passage of the law may be rushed. The ins and outs of what APRA will actually preempt are up in the air—we may still be looking at a federal law that is subject to additional requirements on a state-by-state basis. At this stage, the proposed law contains a number of confusing terms that could ultimately lead to significant litigation if the law passes in its current form. We are still at the early stages. We expect some version of this law to eventually pass, but hopefully the final version resolves more of these issues.

U.S. Privacy Law Round-Up: The Rodeo Is a State of Mind

States are continuing to move with purpose in enacting privacy laws this year. Since our last episode, we have seen major developments in Nebraska, Vermont, and Minnesota. Nebraska's Data Privacy Act was signed into law in April and Maryland's Online Data Privacy Act in May, while both Vermont's Data Privacy Act and Minnesota's Consumer Data Privacy Act await signatures by their respective governors as of May 23, 2024.

Nebraska's law will apply to any entity that does all of the following: (i) conducts business in Nebraska OR produces a product or service consumed by residents of Nebraska; (ii) processes or engages in sale of personal data; and (iii) is not a small business (based on the Small Business Administration's definition—this is similar to Texas's threshold for applicability). Unlike certain other state laws (hi, New Hampshire and New Jersey!), there are not thresholds for how many people's personal data a business processes, or revenue thresholds as a whole or from sale of personal data. So, like Texas, Nebraska's law will apply broadly to businesses. Meanwhile, Maryland's law expressly excludes both employees and individuals in the business-to-business context from the definition of a "consumer" covered by the law. Unlike Nebraska, Maryland's applicability thresholds are similar to other states, only applying to companies who conduct business or direct products and services to Maryland residents, and satisfy at least one of the following: (1) annually control or process personal data of at least 35,000 Maryland residents, or (2) process personal data of at least 10,000 consumers and derive at least 20 percent of its gross revenue from selling personal data.

There are several areas where the Nebraska and Maryland laws are similar, including exemptions (for employees, B2B transactions, data subject to HIPAA or FERPA, and entities regulated under GLBA and HIPAA), privacy rights afforded to consumers (including the right to appeal), requirements for transparency and privacy notices, requirements specific to de-identified data, and when a company is required to conduct a data protection impact assessment prior to certain personal data processing activities. Both laws have similar requirements for privacy contract terms as well, but notably, these requirements overlap significantly with the requirements under Europe's General Data Protection Regulation.

The Maryland and Nebraska laws diverge a bit when it comes to enforcement. Nebraska's Attorney General has exclusive authority to enforce that state's law. On the other hand, a violation of Maryland's law is an unfair, abusive, or deceptive trade practice and is subject to the enforcement and penalties set forth in Maryland's deceptive trade practices law.

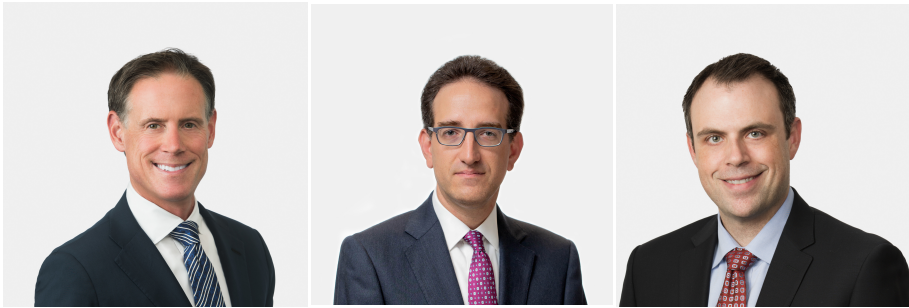
Akerman's **TAKE**

While many of the privacy laws passed by other states overlap significantly, we are starting to see more emerging trends with outliers, such as with applicability thresholds relating to small businesses, global opt-out signals to opt out of sale of personal data, and now enforcement with Maryland's unique approach. Maryland also includes specific prohibitions on certain activities that we aren't seeing elsewhere, such as providing employees, contractors, or processors access to health data unless certain conditions are met, or using a geofence to establish boundaries near certain health facilities. If signed, we anticipate that the Vermont Data Privacy Act will also include unique requirements that don't overlap with other states. And while the American Data Privacy Act has gotten a lot of attention and advanced to full committee consideration (see above), the draft is going to face close examination and scrutiny. As has been the case, companies who are proactive in compliance with foundational privacy principles and in keeping informed of new privacy law developments will find themselves better able to adapt to unique requirements of new privacy 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.

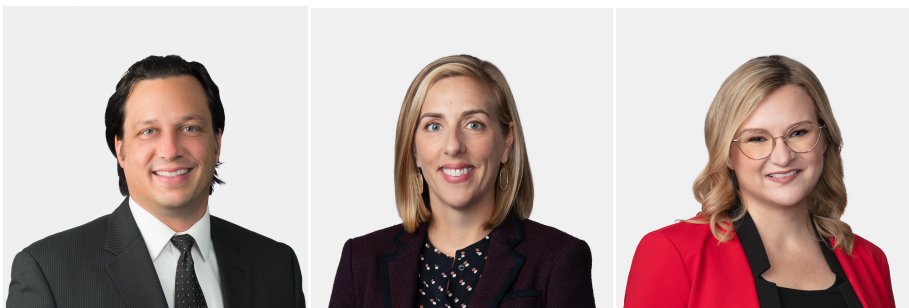
- EXPLAINER THINGS CAST



Bill Heller

Eric Goldberg

Tom Kearney



Tyler Engar

Nora Rigby

Christy Hawkins



**Aliza Pescovitz
Malouf**

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.