

Explainer Things: Episode 3

March 31, 2023



Unless you've been living under a rock, you already know Silicon Valley Bank and Signature Bank failed earlier this month, leading to lots of concern in the banking and fintech industries and wall-to-wall media coverage. To avoid sounding like a rerun when it's only Episode 3, we're not going to cover that well-tread territory here. On the topic of bank runs, though, Mr. Potter asked that we mention we are hearing bad things about the balance sheet over at Bailey Building & Loan. If you bank with Bailey, don't wait until the holidays to move your money: we suggest you do it no later than April 1st.

Also, just prior to press time, the CFPB published the final rule implementing Dodd-Frank Act section 1071, about small business lending data. The rule will require lenders to submit data for closed-end loans, lines of

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 2](#)

[Episode 1](#)

credit, business credit cards, online credit products, and merchant cash advances made by banks, credit unions, and non-depository lenders. The rule covers loans to “small businesses,” defined as businesses with \$5 million or less in gross annual revenue over the previous fiscal year. We’ll have more to say on this in the next issue of Explainer Things.

In the meantime, we continue to bring you 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.

- IN THIS ISSUE - EPISODE 3 -

- To Be or Not to Be, that Is the Question on the CFPB
 - As California Goes, so Goes the Earned Wage Access Nation?
 - Crypto, Crypto, Crypto!
 - Data Breach Notification Requirements: NCUA-Style
 - GAO Slaps the Hand of Federal Regulators: Give Clearer Rules to FinTechs
 - ChatGPT: Predictably Unpredictable, Constantly Changing
 - Continued Coverage on the Rodeo: U.S. State Privacy Law Roundup
-

To Be or Not to Be, that Is
the Question on the



As has been widely reported, the Supreme Court agreed earlier this month to hear a case that will decide whether the CFPB's funding structure is unconstitutional. The Supreme Court will consider whether it agrees with the U.S. Court of Appeals for the Fifth Circuit's 2022 decision that the CFPB's funding structure is unconstitutional, in part, because it is funded by the Federal Reserve and not by Congress. Just last week, the Second Circuit Court of Appeals waded into this murky territory, disagreeing with its sister court and holding the CFPB's funding structure is sound. Now, we have a classic circuit split.

Akerman **TAKES**

It's not a surprise that the Supreme Court agreed to hear the Fifth Circuit case, given the serious implications of that court's decision as to the validity of past and future CFPB actions and potentially the structure of several other federal agencies. We're a bit surprised (or are we?) that the Supreme Court didn't agree to hear the case on an expedited schedule. Given the court's usual timeline, the CFPB's status is likely to remain in limbo until spring or summer 2024. As Tom Petty would tell you if he could (RIP Tom), the waiting is the hardest part. Between now and then, expect any company in active litigation with the CFPB to argue that the agency is unconstitutionally funded in hopes that the Supreme Court ultimately agrees.

As California Goes, so Goes the Earned Wage

Access Nation?



The California Department of Financial Protection and Innovation (DFPI) issued an updated proposal on March 7th that would require earned wage access (EWA) providers in California to obtain a registration or become licensed lenders. The proposal also would require registration by providers of education financing, debt settlement, and student debt relief. This proposal revises a proposal DFPI first issued in late 2021. DFPI believes that registration of these four products is necessary to protect vulnerable consumers.

With respect to EWA, the rule would deem them loans, which California calls “income-based advance products.” If these products have fees that exceed certain restrictions, the provider would be required to obtain a lending license. Otherwise, the provider need only register with DFPI. The proposal would cap fees by converting most fees charged in connection with EWA, except certain subscription fees, to charges included in a usury calculation. Importantly, DFPI would include expedited fees and voluntary tips collected by some providers in this calculation. None of these requirements would apply to EWA programs when funds are advanced directly by an employer.

In explaining its approach, DFPI appears to disregard many arguments that EWA providers have asserted for why their products are not loans, such as the lack of recourse or finance charges, the contractual relationship, and the lack of debt collection and credit reporting. DFPI apparently does not find these elements convincing and instead concluded adequate oversight would be lacking if EWA products were not deemed loans. DFPI also appears concerned that the fees consumers pay for a brief EWA advance, although low in actual dollars, can equate to high APRs when annualized.

Comments on the proposal are due by May 2nd. After that, we expect a pause while DFPI considers the comments and finalizes the rule. We don't expect a final rule until sometime in 2024.

Even if it is never finalized, the impact of this proposal is significant for EWA companies as it is the first determination by any regulator that EWA products are loans. The legal treatment of EWA has been debated in many states and at the federal level. A California final rule could have ripple effects in other jurisdictions that are themselves considering how to treat these products. And, we think there are logical and legal flaws in DFPI's analysis. DFPI looks at EWA in a vacuum rather than in comparison to consumers' other liquidity options – for example, bank overdrafts that can cost \$35 each time and high-cost payday loans. DFPI appears to have neglected the legal requirement to analyze the impact of its rulemaking as it predicts no impact on businesses in the state. It seems to ignore that the rule, if finalized, would force virtually all EWA companies to revise their products and fee structures.

Crypto, Crypto, Crypto!



When we last discussed crypto we noted the hits kept coming for the crypto industry. Unfortunately, the crypto hit parade keeps on marching. On March 23, in an official Investor Alert, the SEC urged investors to “exercise caution with crypto-asset securities,” noting investment in crypto assets can be “exceptionally volatile” and admonishing investors to invest only where they can afford to lose the entire

investment. One day prior, the SEC issued a Wells notice recommending enforcement against Coinbase for alleged violations of federal securities laws regarding its listed digital assets, its staking service Coinbase Earn, Coinbase Prime, and Coinbase Wallet. Coinbase retorted strongly: “We asked the SEC for reasonable crypto rules for Americans. We got legal threats instead.”

These events come on the heels of SEC enforcement actions against other well-known crypto giants, including Gemini and Genesis, Kraken, and industry executives Justin Sun (TRON and BitTorrent) and Do Kwon (Terraform). In this month’s (March) series of unfortunate events, the SEC filed another 5 enforcement actions against crypto-related enterprises and individuals, adding to an already-significant total. Among the more interesting is a suit against Justin Sun and his companies implicating fan-favorites Lindsay Lohan and Jake Paul, who were charged (along with six less-famous others) for allegedly failing to disclose they were compensated for supporting Sun’s products. This month’s SEC filings also detailed multiple charges of alleged fraud against lesser-known crypto companies and individuals, including alleged \$850 million and \$100 million crypto schemes.

The SEC isn’t the only regulator going after crypto companies. The CFTC charged Binance and its founder, Changpeng Zhao, earlier this week with “willful evasion of federal law and operating an illegal digital asset derivatives exchange.” And earlier this month, the New York DFS inked a consent order with BitPay, Inc., for alleged violations of New York’s cybersecurity regulation.

Akerman TAKES 

We get it – crypto is complicated, can be confusing, and requires a lot of work. But the SEC’s regulation-by-litigation approach is the wrong one for the legitimate crypto companies it

is targeting. Sure, there may be some actual bad actors out there whom the SEC should sue, but for the legitimate companies (i.e., the ones not committing fraud) isn't the better approach to clarify the existing fuzzy rules before punishing companies for interpreting the rules in reasonable ways? It would be like an NBA official secretly changing the rules during a close game, causing one team to lose due to the change. C'mon, who would stand for that? Go Mavs! Here's a novel idea, why not be transparent about what the rules are and include the players in the discussions on what they can expect?

Also, it's a lot to ask of Joe Public to differentiate between the alleged fraudsters being sued by the SEC and the credible platforms and services legitimately invested in crypto. The end result is the SEC throwing shade on all crypto, legitimate or not. Well, SEC, in the famous words of Tommy Eagan, "You want sh*& done the way you want sh*& done, you're gonna have to get them hands dirty." Provide the rules before you enforce them.

At the end of the day, the SEC probably isn't reading Explainer Things, but you are. So, at the risk of sounding like a broken record, if you are a crypto business and haven't already, now is the time to review and perhaps bolster your due diligence plans. Don't wait, because the regulators clearly aren't holding back.

Data Breach Notification Requirements: NCUA-Style



Earlier this month, the National Credit Union Administration (NCUA) adopted a final rule requiring

that federally insured credit unions notify NCUA within 72 hours after reasonably believing that a reportable cyber incident has occurred. The rule takes effect in September of this year. The required notice is meant to serve as an early alert from the NCUA, so credit unions do not need to provide a full assessment of the incident within 72 hours (thankfully – since this usually is not possible). The NCUA has indicated it will provide additional reporting guidance before the rule becomes effective.

Akerman **TAKES**

For credit unions that have specific procedures on what notifications are required for a data security incident, it's time to update and dust them off to account for this new requirement. For those who have notification requirements for different sectors, vendors, customers, or other regulators, one effective way to manage them can include an extra procedure to append to your existing incident response plan. Treating the notification requirements and details this way can help organize the chaos by providing the information in one place for first responders, while still being nimble enough to adapt to the ever-changing requirements.

GAO Slaps the Hand of Federal Regulators: Give Clearer Rules to FinTechs

The Government Accountability Office (GAO) issued a report earlier this month on the regulatory landscape of fintech products and their benefits and risks to consumers. The report focused on four specific products: digital deposit accounts, credit builder products, small dollar loans, and earned

wage access (see more on EWA above). It identified both potential risks and benefits for each product, with a particular emphasis on the risks and benefits to unbanked and underbanked consumers. It also summarized the last few years of actions by state and federal regulators to address some of the regulatory uncertainty in the fintech market.

The GAO made only one formal recommendation in the report—to the CFPB concerning earned wage access. In 2020, the CFPB issued an advisory opinion stating that employer-sponsored EWA products are not credit covered by the Truth in Lending Act (TILA) as long as the consumer/employee pays no fees for the product. The GAO recommended that the CFPB clarify whether earned wage access is credit covered by TILA when provided directly to consumers and not through an employer or when fees are charged, among other variations. According to a February 2023 letter from CFPB Director Chopra cited in the report, the agency agrees that the 2020 opinion created confusion, rather than clarity, and has committed to providing “further clarification.” Though not a separate recommendation, the report also criticized the FDIC, OCC, and Federal Reserve for failing to provide sufficient guidance to banks on the appropriate use of alternative data in underwriting when partnering with fintech companies. The GAO recommended back in 2018 that those agencies issue guidance on that topic.

Akerman **TAKES**

First, did you know that GAO is required to issue a yearly report to Congress on the state of financial regulation? Umm, yeah, we did, too. Also, you might not believe us but this report is actually a great read: it's a clearly written primer on how fintechs work and the current legal landscape that applies to them.

The headline from the report is that EWA

companies should expect the CFPB to weigh in soon on whether certain versions of the product are covered by TILA. Then again, the CFPB said it was coming soon last summer ... but crickets. Is the California EWA rulemaking noted above a harbinger of CFPB guidance to come?

Separately, we are not holding our breath that the FDIC, OCC, and the Fed will actually issue the guidance GAO is calling for on alternative data. In our experience, GAO recommendations to federal agencies have about the same impact as the teacher in a Charlie Brown cartoon.

More broadly, while fintech companies often tout their products as beneficial to underbanked consumers, the report noted that there is very little data on whether that segment of consumers actually uses fintech products. The lack of data seems like an opportunity for any fintech companies who do benefit underbanked consumers to share that information with a regulator or academic.

ChatGPT: Predictably Unpredictable, Constantly Changing



For those of you who haven't yet experienced OpenAI's ChatGPT for yourselves, you're in for a unique experience. ChatGPT is one of the first AI models that's been widely available to and used by the public. OpenAI provides users with an AI model that interacts with humans in a conversational way, allowing it to answer follow up questions, admit mistakes, challenge incorrect premises, and reject inappropriate requests. As more people try and report on ChatGPT, we also learn that it can hallucinate and lie. So, we take things with a grain of salt here. But along with OpenAI's release of an updated chat model – called GPT-4 – OpenAI

released a technical paper with a treasure trove of information, including how this model is trying to hallucinate and lie less. We've all seen a flurry of activity in the AI sphere lately, so stay tuned for more updates.

Akerman **TAKES**

OpenAI's GPT-4 technical paper addressed a host of fascinating issues beyond lying and hallucinations. Diving into this page-turner, readers will find details on risks like bias, cyber, phishing, and privacy problems, some of which stem from how the machines learn from data and from one another, and others from how humans interact with the chat model. But there are also some fascinating details for folks who want to learn more about the mechanics of it all – the technical paper is a good resource for learning more about how GPT-4 is trained and the techniques used to improve the model. It is recommended reading for anyone who has caught the AI bug.

P.S. We asked Chat GPT to write a haiku on data privacy and it came up with this gem, which is a lot better than what we could have written...

Data held in trust,
Silent theft, a breach of faith,
Privacy must thrive.

Continued Coverage on the Rodeo: U.S. State Privacy Law Roundup



For the next U.S. state to pass a comprehensive privacy law, we present to you: IOWA. On March 28, Iowa passed Senate File 262, which will become

effective January 1, 2025. Similar to the laws in Connecticut, Colorado, Virginia, and Utah (the “Non-California States”), the Iowa bill addresses a business’s obligations to provide a privacy notice and allow for consumers to exercise their rights in their personal data, and contains contract requirements for any vendors handling personal data of Iowa residents. Also like the Non-California States, Iowa’s privacy law has special rules for collecting, using, and sharing sensitive personal data, which generally includes demographic information (such as racial or ethnic origin, religious beliefs, mental or physical diagnosis, sexual orientation, and citizenship or immigration status), genetic and biometric data, children’s data, and precise geolocation. Under the Non-California States’ laws, businesses need to be prepared to handle this personal data differently, in particular making sure they have the ability to limit use and sharing of sensitive personal data that isn’t necessary to provide goods or services to the consumer. Unlike some of the other privacy laws, Iowa does not give consumers a right to correct their personal data, and Iowa gives businesses 90 days, rather than the 45 days allowed for the other states, to respond to a consumer privacy request.

Among other notable developments, the Colorado attorney general’s office announced earlier in March that it has finalized the rules that will complement the Colorado Privacy Act (the CPA Rules). The CPA Rules include more specific privacy notice requirements than some of their other state counterparts and imposes data minimization obligations on businesses for photos and voice recordings, among other things. There are also detailed requirements for consent, including when it is needed and what is required for valid, informed consent. The attorney general’s press release said the rules will be published in the Colorado Register this month, and will become effective at the same time as the Colorado Privacy Act itself: July 1, 2023.

Akerman **TAKES**

For those of you following along at home, we've already had plenty of privacy activity in the first quarter of 2023. In addition to the 19 other states with active, comprehensive privacy bills, many others are considering topic-specific bills that would handle areas like children's privacy and biometrics. We expect this to be a busy year for the states, and possibly for the federal government, when it comes to privacy legislation.

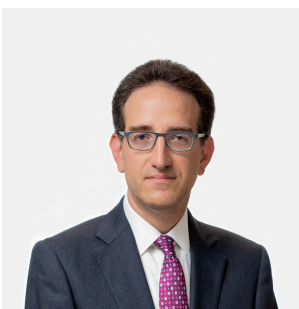
Explainer Things is brought to you by the Consumer Financial Services, Data & Technology Practice Group (CFS+) at Akerman LLP.

For questions about the items in this issue, please contact us at explainerthings@akerman.com.

— EXPLAINER THINGS CAST —



Bill Heller



Eric Goldberg



Tom Kearney



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.