PAUL HASTINGS

Top PHive

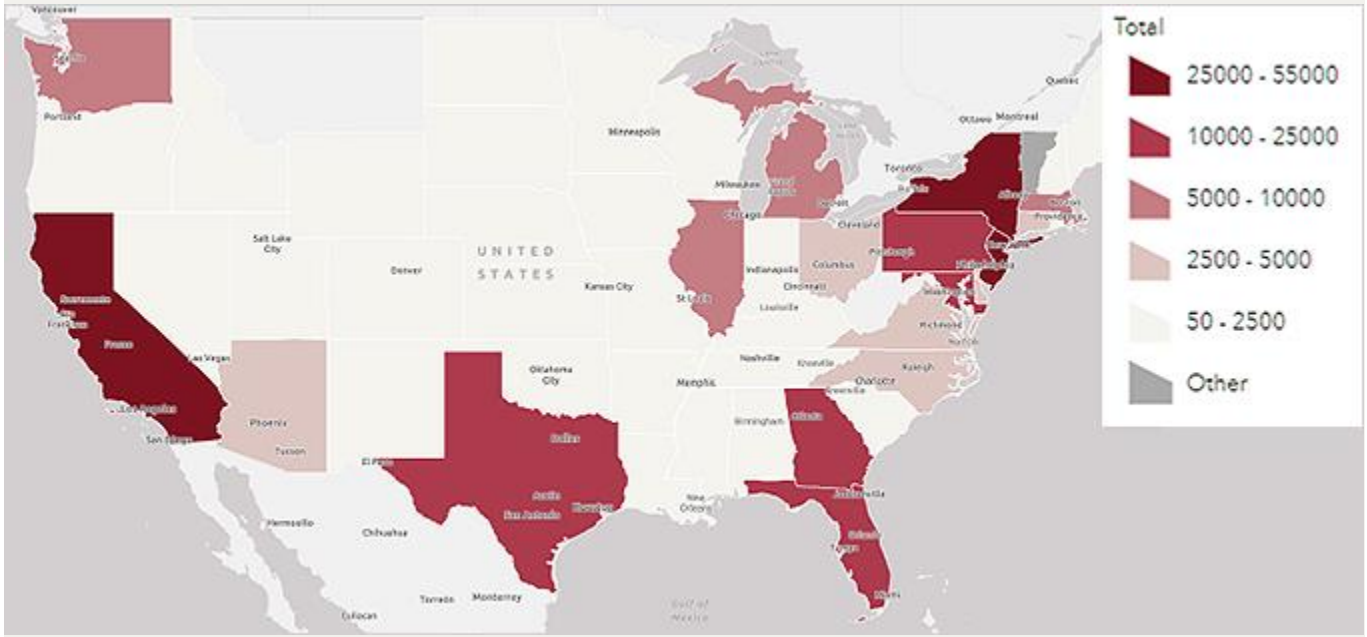
Crypto Enforcement Notes

November 2022

It certainly feels like a race between innovation and enforcement these days, with regulators and law enforcement stepping up the cautionary rhetoric and promising broader enforcement aimed at corporate actors. In October, we saw the first coordinated enforcement action against a cryptocurrency company by OFAC and FinCEN, although one may wonder whether that is as noteworthy as it seems given that they are sister agencies within the Treasury Department and these were still two separate investigations. It does raise some questions about piling on, however. Read those actions closely for takeaways on the government's view on vendor management, "privacy" or anonymity-enhanced coins, and the calibration of compliance measures to transaction growth. Then read below for commentary on the current enforcement temperature impacting the cryptosphere from DOJ, the CFPB, and OCC.

1. **"Reset, Recalibrate," and "Don't Chase" – Acting Comptroller of the Currency Michael Hsu Doesn't Believe the Crypto Hype**
2. **Is the CFPB Out for the Count?**
3. **Cryptocurrency Transactions Play a Role in KleptoCapture Prosecution**
4. **AML Enforcement Wisdom from the Las Vegas Desert**
5. **Corporate Crime Remains Top of Mind for the Justice Department**

CRYPTO SARS COUNT BY STATE (2018-PRESENT)



Source: https://www.fincen.gov/reports/sar-stats

1. "Reset, Recalibrate," and "Don't Chase" – Acting Comptroller of the Currency Michael Hsu Doesn't Believe the Crypto Hype

Acting Comptroller of the Currency Michael J. Hsu was back with another set of noteworthy speeches in October – this time focused on crypto. Last month's Top PHive Crypto Enforcement Notes chronicled Hsu's comments on the proliferation of Bank-Fintech partnerships, and how the OCC (and other Federal Regulators) are using new and available data sources to identify trends suggesting non-compliance. In remarks at DC Fintech Week and the Roundtable on Institutional Investors and Crypto Assets at Harvard Law School this month, Hsu wasn't afraid to show his skepticism of crypto, especially when it interacts with traditional finance or "TradFi." Nor did he mince words in questioning why crypto still attracted a "disproportionate amount of attention and suck[ed] the oxygen out of the room," despite the recent failure of several crypto projects, and associated crash in the crypto markets. Hsu related advice that he had received from his father to not "chase," and pointed to "FOMO" – the fear of missing out – as driving a lot of the attention, despite the fact that in his view, "more pressing things, including the role of non-crypto financial technologies in banking" should take center stage for regulators and policy makers.

Nonetheless, he did elaborate on how crypto platforms and products should be brought "into the regulatory perimeter." In his speech at Harvard Law School, the Acting Comptroller identified three specific areas where supervisory expectations should be clarified in the near term: (1) liquidity risk management of deposits from crypto-asset companies, including stablecoin issuers; (2) finder activities, especially related to crypto-trade facilitation; and (3) crypto custody.

Hsu's comments at DC Fintech Week honed in on three, at times overlapping, "lenses" that may indicate risks to consumers and financial systems more generally. First, Hsu discussed how "skeuomorphism," or crypto's mimicry of

TradFi concepts (such as ownership, custody, or "crypto savings accounts") are used to market products to consumers by creating a façade of the familiar, even though consumers may not actually understand how those concepts are implemented in the crypto space. Second, consistent with his remarks last month, the Acting Comptroller warned that the integration of crypto and TradFi, while promoted as an answer to a range of problems in the financial system, also has potential for cross-contagion and systemic risks. Here, Hsu criticized such promises as ringing hollow considering the "lack of clarity on basic things like ownership, the ever-changing landscape of consensus mechanisms and technology, and the unabating volume of scams, hacks, and fraud." Finally, Hsu pointed to the use of data to manage and identify risks, including the fact that the OCC is considering developing enhanced supervisory processes to better "understand the prevalence and scope of crypto-asset exposures and interconnectedness" at the banks it supervises.

As he did last month regarding Bank-Fintech partnerships, Hsu doubled down on the need for "collaboration and coordination" through information sharing among financial regulators to ensure consumer protection and the safety and soundness of the banking system. He again highlighted the need to gather and monitor data from crypto firms and platforms, especially insofar as those activities interact with TradFi. Hsu suggested this monitoring could be conducted by the Office of Financial Research, and highlighted the OCC's coordination with the FDIC, the Federal Reserve, state banking supervisors and policy makers, as well as international regulators at the Basel Committee on Bank Supervision.

It is no secret that Hsu is a crypto-skeptic. Yet despite this skepticism, Hsu acknowledged that "[b]lockchains and tokens are here and likely to stay" and that regulators need to develop risk-based regulatory "guardrails and gates" so that they do not stand in the way of innovation and progress. What exactly those guardrails and gates are remains to be seen. For now, the OCC seems inclined to remain involved in the regulatory steeplechase, especially when crypto companies (or FinTechs more broadly) interact with TradFi systems or consumers. (Contacts: Ben Seelig, Braddock Stevenson, and Laurel Loomis Rimon)

2. Is the CFPB Out for the Count?

The CFPB has just recently started rattling its sword about cryptocurrency, with Director Chopra making statements this fall reflecting his view that blockchain transactions are within the agency's remit. Although we have yet to see any supervisory or enforcement activity directly targeting a cryptocurrency platform by the CFPB, we know the Bureau is highly focused on emerging payment systems, and is likely to concentrate on companies that facilitate or handle the cash on and off-ramps to cryptocurrency transactions.

So, when the Fifth Circuit ruled in *Community Financial Services Association, Ltd. v. Consumer Financial Protection Bureau* on October 19 that the CFPB's funding structure violates the Constitution's Appropriations Clause and separation of powers principles, many questioned whether that means the CFPB no longer poses a realistic enforcement threat to cryptocurrency businesses. Is the CFPB now out for the count?

By way of background, when the CFPB was created pursuant to the Dodd-Frank Act in 2010, it was funded by a process that involves annual requests by the Bureau to the Federal Reserve, rather than through direct congressional appropriations. The Federal Reserve (which is itself funded outside of the congressional appropriations process through bank assessments), in turn is obligated to provide the funds requested (subject to a statutory cap) out of its own budget. Although there are a number of other federal agencies and programs that are not dependent on congressional appropriations, including the OCC, FDIC, NCUA, and FHFA, most federal agencies' budgets are determined through an annual appropriations process that allows Congress to oversee and approve spending.

In making its ruling, a three-judge panel of the Fifth Circuit specifically invalidated the Bureau's 2017 Payday Lending Rule because, "without its unconstitutional funding, the Bureau lacked any other means to promulgate the rule. Plaintiffs were thus harmed by the Bureau's improper use of unappropriated funds to engage in the rulemaking at issue." Naturally, this raises the question of whether, and to what extent, other supervisory, rulemaking, or enforcement actions could be invalidated on the same basis.

Obviously, the Fifth Circuit's ruling poses existential questions for the Bureau, and we expect the CFPB to challenge this ruling, whether by seeking a rehearing *en banc* before the Fifth Circuit (which may be difficult to obtain given the current composition of the court) and/or with a *certiorari* petition to the Supreme Court. Notably, six district courts and the D.C. Circuit have previously reviewed the CFPB's funding mechanism and found it to be constitutional. Another option would be to seek a legislative fix, bringing the CFPB within an appropriations process and ratifying the Bureau's prior actions, although this would likely be a challenge in the current political environment.

What does this mean for companies who anticipate, or are in the middle of, enforcement proceedings with the CFPB? We do not expect a significant change in approach from the CFPB while these issues are pending, although parties in the Fifth Circuit may see some softening of positions by the Bureau in an effort to avoid drawing challenges to the Bureau's authority. Outside the Fifth Circuit, it will generally be business as usual, but there will be more widespread challenges to the Bureau's authority on this and other bases, and companies may have a general willingness to push back more strongly on excessive or unreasonable demands from the CFPB. We have already seen two companies in active litigation with the Bureau in the Seventh and Ninth Circuits raise new arguments seeking to invalidate the Bureau's actions based on the Fifth Circuit's decision.

Bottom line, this successful challenge to the Bureau's funding structure, along with the Supreme Court's 2019 ruling in *Seila Law, LLC v. CFPB* on the unconstitutionality of limits on the President's ability to remove the CFPB's single Director, are likely to lead to some restructuring, bringing greater congressional oversight and perhaps moderating the impact of any one Director. When it comes to the Bureau's investigations and enforcement actions, the Bureau's vulnerability in this area will provide respondents, including any cryptocurrency companies being targeted, the opportunity to press harder against Bureau overreach. (Contact: Laurel Loomis Rimon)

3. Cryptocurrency Transactions Play a Role in KleptoCapture Prosecution

A 12-count indictment was unsealed on October 19 in the Eastern District of New York, bringing to light a prosecution by the DOJ, FBI, Department of Commerce's Office of Export Enforcement, and the DOJ's Task Force KleptoCapture. While this prosecution is not primarily focused on cryptocurrency activities, it reflects how cryptocurrency transactions play a significant role in a broad range of illicit activity that is squarely in the focus of law enforcement.

Seven defendants, including individuals from Russia, Spain, and Venezuela, were indicted in connection with a global procurement, smuggling and money laundering network operating since at least 2018. The government alleges that the defendants used a German company as a front for a black market scheme to sell embargoed oil belonging to Venezuela's state-owned Petróleos de Venezuela SA (PdVSA), as well as sensitive dual-use equipment subject to military uses, to Russian and Chinese end users in violation of U.S. sanctions and export controls. Two of the defendants have been arrested abroad and are subject to extradition proceedings to bring them to the United States.

According to the indictment, "[i]n furtherance of the scheme and to launder the illicit proceeds, the defendants employed a vast network of shell companies and bank accounts throughout the world and utilized cryptocurrencies and bulk cash transactions." More specifically, the co-conspirators are alleged to have used "a variety of methods to make illicit payments and launder criminal proceeds, including (1) a network of shell corporations with bank accounts in various jurisdictions, (2) bulk cash payments through unlicensed money remitters, and (3) cryptocurrency payments."

In connection with multiple payments ranging from hundreds of thousands, to millions of dollars of Tether (USDT) to several different wallet addresses, one co-conspirator told another: "*It's like SMS, and they tell you yes . . . everything is ok, this money is yours. It's quicker than telegraphic transfer, USDT. That's why everyone does it now. It's convenient, it's quick*." (In fact, the indictment is worth a read for a number of very helpful-to-the-government statements captured by the wiretap.) In addition to the criminal charges, the government is seeking forfeiture of the funds involved in the alleged offenses, or substitute property amounting to the same value.

Notably, neither the indictment, nor the DOJ's press release indicate any facts that would suggest compliance failures on the part of any financial institution related to the over four million dollars' worth of cryptocurrency that was identified as part of the money laundering conspiracy. Nonetheless, cryptocurrency companies are expected to take note of prosecutions like this in order to be on the lookout for transactions that may involve the parties named in the indictment and to update their risk assessments and transaction monitoring procedures to account for the type of activity described. (Contacts: Laurel Loomis Rimon and Leo Tsao)

4. AML Enforcement Wisdom from the Las Vegas Desert

In October, ACAMS held its annual conference of AML professionals, regulators and law enforcement in Las Vegas to share knowledge and discuss trends. The event featured keynotes by both Terrorism and Financial Intelligence Undersecretary Brian Nelson and FinCEN Director Him Das which focused on national security issues and the beneficial ownership rule, respectively. Additionally, the annual regulatory panel discussed a broad range of AML topics with representation from the FDIC, OCC, Federal Reserve, FINRA, and FinCEN. While many discussions focused on newly issued or forthcoming regulations implementing the AML Act of 2020, these speakers also made several enforcement-focused statements. In particular, the event focused on themes involving the overlap of OFAC and AML obligations, risks in mergers and acquisitions, and third-party relationship management.

While OFAC and FinCEN have always coordinated on some level, Undersecretary Nelson repeatedly reiterated the importance of OFAC and FinCEN in supporting the administration's response to Russia's invasion of Ukraine. In his remarks and in response to questions, Nelson highlighted OFAC's actions targeting Russian oligarchs and the importance of financial reporting to assist in tracing potential sanctions evaders. Nelson reminded the audience of FinCEN's financial intelligence collection abilities, including its Geographic Targeting Order on Real Estate. FinCEN has also issued multiple advisories to financial institutions encouraging reporting on red flags and suspicious activity that may indicate evasion of Russian sanctions. Director Das also noted OFAC and FinCEN collaboration and made statements suggesting many businesses, including financial institutions, should be prepared for more targeted information reporting requirements. This reporting will provide greater transparency to Treasury in combatting illicit actors and helping identify the U.S. businesses and financial institutions that have facilitated these transactions. While the initial focus will be on tracing Russian oligarch assets, the coordination between OFAC and FinCEN will undoubtedly result in additional compliance investigations.

During the regulator panel and throughout the conference, speakers focused on risk management of third-party relationships. It is clear that this is top of mind for regulators, including the OCC which referred banks to its 2013 guidance on the issue. The tone and content of the regulator panel suggested that these issues are of significant focus within financial regulatory agencies. As we discussed last month, banks and fintechs need to be hyper vigilant in ensuring compliance with laws and regulations when conducting bank business through these partnerships.

Lastly, the FDIC stressed the importance of understanding residual AML and compliance risk from mergers and acquisitions. The FDIC expects that acquiring financial institutions implement policies and procedures to assess and mitigate incoming compliance risk. In particular, banks should ensure that they understand any compliance deficiencies or shortcomings in the target product or institution, assess the impact on the risk profile of the acquiring institution, and develop a plan to address any deficiencies or risks. The FDIC referred the audience to its recent request for information and comment on rules, regulations, guidance, and statements of policy regarding bank merger transactions. Considering that many enforcement actions arise out of the acquisition of a product line or institution with significant risk, banks and other financial institutions should pay particular focus to conducting appropriate due diligence on acquisition targets. With growing consolidation in the banking industry, the FDIC's remarks are particularly on point. (Contact: Laurel Rimon and Braddock Stevenson)

5. Corporate Crime Remains Top of Mind for the Justice Department

Under the Biden Administration, the DOJ has made the prosecution of corporate crime a high priority. To that end, the DOJ has taken a series of steps to combat corporate crime, including adopting new corporate crime initiatives, revising its enforcement policies, and dedicating increased resources. Many of those actions have been aimed at addressing crimes committed by cryptocurrency and other digital asset companies. For example, last year, the DOJ created a specialized team of prosecutors focused on cryptocurrency crimes, and just last month, it announced the creation of a national Digital Asset Coordinator (DAC) Network to "combat the growing threat" of the illicit use of digital assets. In September, Deputy Attorney General (DAG) Lisa Monaco announced a series of additional changes to the DOJ's corporate enforcement policies. While these changes were not specifically aimed at digital asset companies, these companies should, nonetheless, take note of several of these policy changes.

First, the DAG announced new policies that make clear that a strong corporate compliance policy is still one of the most important factors for the DOJ in determining how harshly it will treat a corporate offender. For example, the DAG announced a new policy requiring all DOJ components to make clear the benefits a company will receive if it voluntarily self-discloses its misconduct, including the presumption against a guilty plea. The DAG also announced that when prosecutors evaluate the effectiveness of a corporate compliance program, they will look at whether the company has adopted a compensation system that recognizes the importance of compliant behavior, including salary and bonus clawbacks for employees who engage in misconduct. As the DAG explained, these changes evidence that a company has a positive "culture of compliance."

This focus on compliance is notable because, according to the DOJ, although digital assets present heightened risks for money laundering, sanctions evasion, and fraud, some companies in this sector may be more focused on growth than compliance. Companies that fail to focus on compliance will be exposed to more serious consequences by the DOJ, making it important that cryptocurrency companies emphasize a culture of compliance from the beginning. Compliance programs are not one-sized fits all, however, so an effective program should be tailored to the risk profile of the company, and the program for a growing company need not be the same as for an established one. The DOJ's guidance for corporate compliance programs is a good starting point to understand what the Department expects from a compliance program.

Second, digital asset companies located outside of the United States should be aware of new DOJ policies aimed at prosecuting foreign companies. Specifically, the DAG has now made it harder for companies to claim that foreign data privacy and similar laws prevent them from producing materials while cooperating with the DOJ's investigation. Companies now have the burden of establishing that such laws actually prevent the production of relevant materials, and that there are no workarounds to permit production. The DAG also has now required federal prosecutors to focus on charging foreign individuals. While the DOJ may decide to defer to a prosecution by a foreign jurisdiction, federal prosecutors are required to consider the other jurisdiction's interests and ability to bring an effective prosecution, and the likely consequences of such a foreign prosecution. Together, these provisions reflect that the DOJ's enforcement focus will include digital asset companies operating outside of the U.S.

Third, the DAG announced new policies relating to the use of personal devices and encrypted ephemeral messaging applications, such as WeChat and WhatsApp. In recent years, the DOJ and other U.S. agencies have been focused on the use of such applications to conduct business communications can facilitate corporate crimes. As the DAG explained, such applications pose "significant corporate compliance risks, particularly as to the ability of companies to monitor the use of such devices for misconduct and to recover relevant data from them during a subsequent investigation." Under the new policy, prosecutors are now required to consider whether a company has "implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved." Because employees at many digital asset

companies, and in particular foreign companies, rely upon ephemeral messaging applications, such companies should consider whether their compliance policies have adequately addressed these risks.

As the DAG explained, the DOJ's focus on corporate criminal enforcement will continue, as evidenced by the DAG's statement that next year the DOJ will ask Congress for $250 million for corporate crime initiatives. Digital asset companies should continue to track these changes to mitigate the risk of any unwanted attention from federal law enforcement. (Contact: Leo Tsao and Laurel Rimon)

To receive regular updates, please click here to subscribe to Top PHive Crypto Enforcement Notes.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Laurel Rimon
Partner, Litigation Department
1(202) 551-1889
laurelrimon@paulhastings.com

Leo Tsao
Partner, Litigation Department
1(202) 551-1910
leotsao@paulhastings.com

Braddock Stevenson
Of Counsel, Litigation Department
1(202) 551-1890
braddockstevenson@paulhastings.com

San Francisco

Ben Seelig
Associate, Litigation Department
1(415) 856-7003
benseelig@paulhastings.com