CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

The New Cabinet News and Views

March 10, 2022 | Issue No. 1

Table of Contents:

The Reimagined Cabinet News and Views

Welcome to the first issue of our new, reimagined *Cabinet News and Views*.

Cabinet News and Views will now be published weekly – on Thursdays – with a look back at the week's news related to the financial markets … and ahead at what's coming in the days and weeks to come. We promise to continue to provide the same level of sharp analysis and unsurpassed expertise that you have always received from Cadwalader attorneys – real-world explanations and commentary intended to help you think through and respond to important developments.

Issues of *Cabinet News and Views* will include a few standard features, including:

- **Take Five**: a brief look at five topics that are on the minds of financial services industry participants
- **In Depth**: a deeper dive into timely and important topics
- **Cadwalader Corner Q&A**: interviews with industry leaders and other key influencers

We'd love to hear what you think of our inaugural issue of our new *Cabinet News and Views* and what we can do to make this most valuable to you. Please send your comments and suggestions here.

Happy reading!

Daniel Meade & **Michael Sholem**
Co-Editors, *Cabinet News and Views*

New Biden Executive Order on Digital Assets

By **Christian Larson**
Associate | White Collar Defense and Investigations

President Biden issued an executive order ("EO") yesterday on "Ensuring Responsible Development of Digital Assets." The EO calls for an aligned, all-of-government approach to digital assets, which the EO defines to include, among other things, cryptocurrencies, stablecoins, central bank digital currencies ("CBDCs"), and other representations of value or financial instruments that may be a security, commodity, derivative, or other financial product.

Until now, U.S. government agencies have taken a variety of approaches to digital assets, ranging from watching and waiting to aggressive enforcement of existing regulations designed for traditional finance. This EO is notable because it directs the full gamut of U.S. federal agencies to identify and study opportunities, risks, and potential risk mitigants associated with digital assets, and to propose action plans, regulations, and legislation accordingly.

Recognizing the enormous growth of digital asset offerings and adoption in recent years, a key theme in the EO is that the United States should take strong steps now to maintain its leadership in the global financial system. The EO calls upon agencies to explore and harness the potential benefits that digital assets may offer – for example, in terms of cheaper, faster, and safer funds transfers – while ensuring that the US maintains the economic and national security benefits it derives from the central role of the U.S. dollar in global finance.

The EO calls upon U.S. government agencies to work through defined interagency processes to prepare a variety of detailed reports to the President. The mandated reports fall under six key topics: consumer protection, financial stability, illicit activity, U.S. competitiveness, financial inclusion, and responsible innovation. With report deadlines ranging from 90 days to one year, the next 12 months will see an unprecedented level of U.S. government engagement on digital assets.

Federal Reserve Board Re-proposes Guidelines for Access to Federal Reserve Bank Accounts and Services

By **Daniel Meade**
Partner | Financial Regulation

On March 8, the Federal Register published the Federal Reserve Board's supplemental notice and request for comment on updates to its proposed guidelines for Federal Reserve Banks to utilize in evaluating requests for access to Reserve Bank master accounts and services. The supplemental notice includes a new section of the proposed Guidelines that would establish a three-tiered review framework on the level of scrutiny to be applied to requests for Reserve Bank accounts and services.

The re-proposal keeps the same six principles from the original proposal, and adds a section 2 to the original proposal, which would establish a three-tier framework for the review process for different types of institutions.

- Tier 1 review would generally be less intensive and more streamlined. It would only be available to consist of eligible institutions that are federally insured.
- Tier 2 review would generally be an intermediate level of review. It would apply to eligible institutions that are not federally insured but (i) are subject (by statute) to prudential supervision by a federal banking agency; and (ii) any holding company subject to Federal Reserve oversight (by statute or by commitments).
- Tier 3 review would generally be the strictest level of review. Tier 3 institutions consist of eligible institutions that are not federally insured and not subject to prudential supervision by a federal banking agency at the institution or holding company level.

Reserve Bank account access might often be viewed as not particularly noteworthy. However, it comes against the backdrop of more and more crypto-currency exchanges or custodians seeking access to Reserve Bank accounts and services to better integrate with the payments system. It also comes as the nomination of Sarah Bloom Raskin to be a Fed Governor and the Vice-chair of Supervision has stalled in light of her service on the board of directors of a fintech firm that is one of the only such firms to have received a Reserve Bank master account. Thus, the proposal is likely to get more interest from a wider array of stakeholders.

Strengthening Cybersecurity Notification Requirements

By **Keith M. Gerver**
Associate | White Collar Defense and Investigations

Last week, the U.S. Senate passed S. 3600, the Strengthening American Cybersecurity Act, which represents a significant step forward in the establishment of a national data breach notification law for certain critical infrastructure businesses and marks, for the first time, that businesses will be required to report when they have made ransomware payments.

Here are five key takeaways from the bill:

- Under the bill, a "covered entity" will be required to report certain cyber incidents they experience to the Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours of when the "covered entity reasonably believes that the covered cyber incident has occurred," and any ransom payments they make as a result of a ransomware attack not later than 24 hours after the payment has been made.

- The bill delegates to the CISA Director the responsibility to determine via notice-and-comment rulemaking which businesses in any of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (to include, among others, commercial facilities, financial services, and healthcare and public health) are covered entities.

- Only "*substantial* cyber incidents" must be reported, and the bill delegates to the CISA Director the responsibility to define via rulemaking what those incidents are. At a minimum, they must be cyber incidents that *actually* jeopardize information on information systems or the systems themselves.

- If the CISA Director has reason to believe that a covered entity has failed to make a required report and has not responded (or responded adequately) to a request for information, the bill gives them the authority to issue a subpoena to compel disclosure. If the covered entity does not respond to the subpoena, then the CISA Director may refer the matter to the Attorney General to bring a civil action to enforce it.

- Covered entities that submit required reports enjoy liability protection from any action brought against the covered entity solely based on the submission of a required report.

The House of Representatives attempted, but failed, to include similar language in the annual defense authorization bill that it passed in December 2021. Nevertheless, after years of discussion and debate over the creation of a mandatory federal data breach reporting regime, the volume and tempo of cyberattacks against critical infrastructure businesses appears finally to have reached a level where opposition in private industry has significantly softened. We should expect to see legislation signed into law this year.

EU AML List Will Add The Cayman Islands

By **Michael Sholem**
Partner | Financial Regulation

On February 21, 2022, Commission Delegated Regulation[1] was published in the Official Journal of the European Union which will add the Cayman Islands to the list of countries that have been identified by the European Commission as having strategic anti-money laundering ("AML") and counter-terrorist financing ("CTF") deficiencies (the "EU AML/CTF List"). This new law, and the changes to the EU AML/CTF List, will take effect on March 13, 2022. This listing is linked to the Cayman Islands having been added to the Financial Action Task Force ("FATF") "greylist" of jurisidictions under increased monitoring in June 2021, prompting the European Commission to assess whether the Cayman Islands should be added to the EU AML/CTF List.

From March 13, 2022, EU AML laws will require financial services businesses in the EU to apply enhanced due diligence measures when entering into business relationships with Cayman established entities. Given the long lead time since the FATF announcement, most institutions have already put in place systems and controls to ensure that such enhanced due diligence is carried out.

Furthermore, the EU Securitization Regulation prohibits the establishment of a "securitisation special purpose entity" ("SSPE") in any country that appears on the EU AML/CTF List. Accordingly, EU investors will be prohibited from investing in securitization instruments issued by SSPEs established in the Cayman Islands, and could potentially face penalties from EU national regulators if they do so.

We note that there is a divergence between the EU and UK securitization regimes, as the UK Securitization Regulation does not contain a post-Brexit amendment referencing the EU AML/CFT List for the prohibition. Instead, the UK law refers only to a prohibition of the establishment of SSPEs established in FATF "blacklist" jurisdictions (currently North Korea and Iran).

There remains some uncertainty about the market effects of this development, particularly in relation to Cayman Islands-issued securitization instruments issued prior to March 13, 2022. Nevertheless, it is clearly the case that where transactions are to be marketed to EU investors, an alternative offshore jurisdiction for the SSPE will need to be used.

[1] Delegated Regulation (EU) 2022/229, which amends Delegated Regulation (EU) 2016/1675 on the list of high-risk third countries with strategic anti-money laundering and counter-terrorist financing deficiencies under the Fourth Money Laundering Directive ((EU) 2015/849), available here.

LIBOR Federal Legislation Takes Big Step Forward

By **Lary Stromfeld**
Partner | Financial Regulation

Federal legislation addressing the transition of legacy LIBOR contracts took a big step forward when it was included in the Omnibus bill passed late last night by the House of Representatives.

The bill would provide legal certainty for legacy contracts with inadequate or unworkable "fallback provisions" when USD LIBOR stops being published in June 2023. For contracts with no fallback for the LIBOR rate, the legislation would automatically impose a rate selected by the Federal Reserve based upon the Secured Overnight Financing Rate (SOFR). The legislation also includes a safe harbor against liability for parties with contractual discretion who choose the Federal Reserve's SOFR-based rate to replace LIBOR.

The Federal Reserve has until 180 days after enactment of the legislation to issue regulations carrying out its provisions. Market participants are reminded that the legislation is a "safety net" for legacy LIBOR contracts that are not refinanced or amended to address the discontinuation of LIBOR. Regulators have made clear that they recommend proactive remediation of legacy LIBOR contracts.

In Depth: Listen to Your Regulator on Sanctions and Crypto

By **James A. Treanor**
Special Counsel | White Collar Defense and Investigations

It should come as no surprise that the crushing sanctions imposed on Russia in recent weeks will be met with efforts to evade their impact. From Russian firms starved for U.S. dollars to oligarchs starved for that new villa or yacht, some sanctions targets inevitably will attempt to access the capital, goods and services from which they have been severed so completely since Russia's invasion of Ukraine began. To do so, in most cases they will be forced to conceal their involvement in a transaction. Enter: crypto.

Almost immediately after the conflict erupted, concerns were raised by pundits and policymakers that cryptocurrencies – by virtue of their decentralization and the anonymity they afford – could turbocharge efforts to evade the massive package of sanctions imposed on Russia. For example, in a March 2 letter, Senators Elizabeth Warren and Mark Warner wrote to Secretary of the Treasury Janet Yellen asking for information on how Treasury intends to "inhibit the use of cryptocurrency for sanctions evasion."

In response to these alarm bells, industry experts have observed that, in fact, digital currencies are unsuitable to sanctions evasion. For starters, crypto is arguably too small to accommodate widespread sanctions evasion – that is, there is simply not enough cryptocurrency available to facilitate the systematic evasion of sanctions against a country like Russia, which has the world's eleventh largest economy.

In addition, sanctions evasion, like other forms of money laundering, demands obscurity and non-traceability. Cryptocurrency – for all the talk of anonymity and decentralization – has transparency and traceability literally built into its DNA. A blockchain is, after all, a public and immutable record of all transactions. Even if identities are not attached to those transactions, authorities are increasingly adept at putting names and faces to the blockchain's ones and zeroes. Witness the DOJ and FBI's successful effort to recover millions of dollars in bitcoin ransomware payments, and the arrest of two New York residents who stole and unsuccessfully attempted to launder approximately $4.5 billion in cryptocurrency.

These arguments against cryptocurrency as an effective tool of sanctions evasion undoubtedly have merit. But for exchangers, administrators, wallet providers, and others involved in the industry, they risk missing the point. First, there is little doubt that cryptocurrency can be – indeed, has been – used to evade sanctions, even if not on a massive scale. More importantly, the U.S. government has in recent months repeatedly highlighted legal risks associated with cryptocurrency, including in connection with sanctions evasion. Last fall, OFAC released some of its most detailed compliance guidance ever, devoted entirely to sanctions risks in the cryptocurrency industry. The following month, in its anticipated Sanctions Review, one of Treasury's central messages was that cryptocurrencies and other

technologies may provide bad actors with “new ways of hiding cross-border transactions” and thereby “reduce the efficacy of American sanctions.”

More recently, on March 1 – soon after large-scale Russian military action began – President Joseph R. Biden announced in his State of the Union Address the formation of a DOJ-led initiative “to go after the crimes of Russian oligarchs.” In an announcement released the following day, DOJ made clear that one mission of the new “KleptoCapture” task force would be to target “efforts to use cryptocurrency to evade U.S. sanctions.” Most recently, FinCEN warned financial institutions on March 7 to “be vigilant about potential Russian sanctions evasion, including by both state actors and oligarchs.” The notice also underscored that “CVC [convertible virtual currency] exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons.” And most recently, President Biden’s March 9 Executive Order underscores that understanding and managing the potential threats posed by cryptocurrency will be an all-of-government effort, and a key area of focus for the administration going forward.

The clear message, then, is that regardless of the actual viability of cryptocurrency as a means of evading sanctions, OFAC, DOJ, FinCEN, and other enforcement agencies will be looking hard for violations. Whether many or few, the U.S. Government will find violations, and those involved – including financial institutions, exchangers, wallet providers, and other market participants – will be held accountable. Firms that do not heed their regulators’ repeated warnings to understand the risk environment, appropriately diligence users, and implement other suitable controls may soon regret it.

Cadwalader Corner Q&A: BNY Mellon's Jason Granet

Jason Granet is the Chief Investment Officer at BNY Mellon, responsible for managing the firm's securities portfolio as well as BNY Mellon's LIBOR transition efforts. Prior to joining BNY Mellon in 2021, Jason spent more than 20 years at Goldman Sachs across a variety of leadership roles, including head of Goldman Sachs' global LIBOR transition.

The Federal Reserve is expected to hike interest rates at its upcoming policy meeting. What do you envision will be the impact of that decision?

Many of the Fed's significant actions over the last two years were related to the economic impact created by COVID-19. But now we have this inflation backdrop, and the Fed is starting to tighten policy.

As we all know, this is a particularly challenging environment when you consider supply chain issues and the geopolitical conflict in Ukraine. With people now paying upwards of $5 per gallon of gas and with the rising cost of food, typically you would have a Fed policy that makes it easier on people.

It's not that simple, though. These global challenges have injected very significant amounts of volatility into the markets. You have some people that think rates are going to go higher in the short term. You have others that think we're going to go into a recession because Americans are not going to be able to afford heightened costs of living. Therefore, the future state of the world right now and the flow of commodities is very unknown.

How does someone in charge of a large investment portfolio make decisions in this kind of environment?

My approach is to be over-sensitive to your shortcomings and blind spots. You have to be humble and admit that you don't know everything. Stay with things that you understand and avoid areas where there's a good amount of uncertainty.

What are some of the trends BNY Mellon is most excited for in the future of capital markets?

We're highly focused on digital transformation and advanced technology: blockchain, AI, and machine learning. We're building the industry's first platform

that bridges digital asset custody, execution and administration seamlessly with traditional assets.

We also recognize transparency around ESG as a top priority for the financial world. To that end, we've launched an innovative cloud-based ESG Data Analytics application.

This is a unique moment in financial history, and we see now as the time to adapt and help guide the next chapter for the financial industry.

Tell us something that we might not know about you.

Aside from playing pickleball or basketball, I also have a minor LEGO habit that has turned into something very meaningful and special. I'm a trustee of a charity called Fairy Bricks, which donates LEGO sets to hospices and hospitals, brightening the lives of sick children. From humble beginnings and a single hospital donation in 2012, we now aim to deliver LEGO to over 200 hospitals throughout the UK and 26 other countries per year. In fact, we're finalizing some details now to send nearly 20,000 LEGO sets to refugee families in Europe.
