

Cabinet News and Views

Informed analysis for the financial services industry



So Long, Summer

September 1, 2022

Table of Contents:

- [In This Issue ...](#)
- [FDIC Issues Guidance on NSF Fees for Multiple Re-presentments](#)
- [FBI Warns About Cybersecurity Problems on DeFi Platforms](#)
- [DOJ Opines on FDIC Board](#)
- [ESMA: Rules for Third Country Benchmarks Are Not Fit for Purpose and Should Be Reviewed](#)

In This Issue ...

We say it every year: how did the summer go by so quickly? Well, it has, and as we approach Labor Day in the United States, we hope all of our readers in the U.S. and Europe can squeeze in a few more summer highlights before we all buckle in for what will likely be a busy September.

Have a great holiday weekend.

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

FDIC Issues Guidance on NSF Fees for Multiple Re-Presentments



By **Daniel Meade**
Partner | Financial Regulation



By **Mercedes Kelley Tunstall**
Partner | Financial Regulation

On August 18, the Federal Deposit Insurance Corporation (“FDIC”) issued [Financial Institutions Letter 40-2022](#) (“FIL 40-2022”), which provided supervisory guidance for state non-member banks and multiple non-sufficient funds (“NSF”) fees. FIL 40-2022 and its attached guidance is similar in content to an issue the FDIC highlighted in its March [Consumer Compliance Supervisory Highlights](#).

The FDIC stated that it is issuing the guidance because of its observations in consumer compliance exams where consumers are charged multiple NSF fees for the same transaction when a merchant resubmits the transaction for payment. The FDIC has also observed that some institutions’ disclosures did not adequately describe the institution’s re-presentment practice. The FDIC stated that such practices could result in being deemed a violation of law in exams as an unfair and/or deceptive practice in violation of [Section 5 of the FTC Act](#).

The FDIC’s guidance encouraged institutions to consider implementing the following practices to mitigate the risks noted in the guidance:

- Eliminating NSF fees.
- Declining to charge more than one NSF fee for the same transaction, regardless of whether the item is re-presented.
- Conducting a comprehensive review of policies, practices, and monitoring activities related to re-presentments and making appropriate changes and clarifications, including providing revised disclosures to all existing and new customers.
- Clearly and conspicuously disclosing the amount of NSF fees to customers and when and how such fees will be imposed, including:
 - information on whether multiple fees may be assessed in connection with a single transaction when a merchant submits the same transaction multiple times for payment;
 - the frequency with which such fees can be assessed; and
 - the maximum number of fees that can be assessed in connection with a single transaction.
- Reviewing customer notification or alert practices related to NSF transactions and the timing of fees to ensure customers are provided with an ability to effectively avoid multiple fees for re-presented items, including restoring their account balance to a sufficient amount before subsequent

NSF fees are assessed.

This guidance from the FDIC is fairly broad, and, interestingly, is not presented as interagency guidance. Arguably, it might have been more likely to see such guidance from the Consumer Financial Protection Bureau or the Federal Trade Commission. The FIL 40-2022 guidance also seems to toe the line (if not go beyond the line) of the federal banking agencies' so-called 2018 [Guidance on Guidance](#) by seemingly giving a list of requirements for state non-member banks under the guise of encouragement. The Guidance on Guidance was codified as a [final rule in 2021](#). For the FDIC, this rule can be found at [12 C.F.R. Part 302](#).

FBI Warns About Cybersecurity Problems on DeFi Platforms



By [Mercedes Kelley Tunstall](#)
Partner | Financial Regulation

Decentralized finance platforms (DeFi) are designed to operate in a decentralized manner primarily through the utilization of smart contracts. Smart contracts are simply a name given to small “if/then” statements written in computer code that are self-executing. Smart contracts are used throughout the cryptocurrency and blockchain space, are an integral component in non-fungible tokens (NFTs), and can allow for things to happen automatically, without human intervention. For example, a smart contract could be coded such that payment for an item could be released upon receipt of a shipment, so **if** the shipment is received, **then** payment is released.

In the case of DeFi platforms, the coded smart contracts allow for trading of cryptocurrency, stocks, and ETFs; funds to be transferred between parties; and even loans to be made that are secured by crypto or other investments. These smart contracts interact with the blockchain, but in most cases are not written to the blockchain, which means that the smart contracts do not enjoy the encryption protection of the blockchain, and are simply computer code that can be manipulated and hacked just like any other computer code, if not properly secured by the DeFi platform. The FBI’s [August 29, 2022 Public Service Announcement](#) warns the public (*i.e.*, investors) about these smart contract vulnerabilities on DeFi platforms. The PSA reports that in just three months of 2022, “cyber criminals stole \$1.3 billion in cryptocurrencies, almost 97 percent of which was stolen from DeFi platforms.”

The FBI recommends that investors should seek advice from a licensed financial adviser, but to the extent DeFi platforms will be used, investors should research the DeFi platforms they are using and ensure that the platform has conducted thorough security audits that include a “code audit” and should be alert, in particular, to “DeFi investment pools with extremely limited timeframes.” Companies that provide DeFi platforms are urged to step up their cybersecurity compliance, to conduct a code audit and to develop a robust incident response plan.

DOJ Opines on FDIC Board



By **Daniel Meade**
Partner | Financial Regulation

The DOJ recently published an [opinion](#) from the Office of Legal Counsel (“OLC”) regarding the FDIC Board. The OLC opinion concluded that “the Chairperson of the FDIC Board does not have the authority to prevent a majority of the Board from presenting items to the Board for a vote and decision.”

This OLC opinion was requested by the current General Counsel of the FDIC. Readers may recall that at the end of 2021, there was a bit of a [power struggle at the FDIC Board](#) on whether the FDIC should proceed with a request for information on Bank Merger Act Guidelines. While a majority of the FDIC board (the three members appointed by a Democrat) were in favor of issuing the request for information, the then-Chair of the FDIC, the sole Republican on the Board at that time, was not in favor of the issuance, and purported to block the issue from the agenda of a board meeting. Chair McWilliams [resigned](#) from the FDIC Board shortly after this disagreement.

The OLC opinion makes clear that most power is vested in the FDIC Board rather than solely in the Chairperson. The opinion could become important again the next time Presidential administrations switch parties and we see a change in the makeup of the *ex officio* members (*i.e.*, the Comptroller of the Currency and the Director of the CFPB).

ESMA: Rules for Third Country Benchmarks Are Not Fit for Purpose and Should Be Reviewed



By **Michael Sholem**
Partner | Financial Regulation

On August 19, the European Securities and Markets Authority (“ESMA”) [announced](#) the publication of its [response](#) to a consultation on the European Commission’s (the “Commission”) proposals to amend the regime for the provision of “third country” (meaning non-EU) benchmarks into the EU under the Benchmarks Regulation (“BMR”). The Commission’s [consultation](#), which concluded on August 12, 2022, asked for views on whether the rules applicable to the use of benchmarks administered in a third country, which will fully enter into application in January 2024, are fit for purpose and if not, how should the BMR’s third country regime be amended. The BMR entered into force in January 2018, however the use of non-BMR compliant third country benchmarks in the EU is still permitted until December 31, 2023 under transitional arrangements.

In its response, ESMA states that its own research has found that there are 330 third country administrators providing benchmarks available to supervised entities in the EU, out of which 3% (*i.e.*, 11) are already authorized to be used in the EU under one of the third country regimes (recognition or endorsement under the BMR). The response goes on to note that 20% of the 330 are exempted in accordance with the BMR’s scope provisions, while the remaining 77% of those third country administrators provide benchmarks that are not yet subject to the regulation. ESMA concludes that should “administrators not apply for recognition or endorsement before the expiration of the transitional period, hundreds of thousands of benchmarks will not be accessible anymore to EU supervised entities and thus for use in the EU, which could be detrimental to the functioning of the EU financial markets.”

ESMA expects that the larger third party administrators based in third countries would be willing to apply in the EU and that this would “include more likely the UK-based administrators, which were already subject to BMR before the UK left the EU.” However, ESMA expresses uncertainty that small or medium administrators would apply for recognition or endorsement before the expiration of the transition period. ESMA said that, in such a scenario, while the extent of the use of these benchmarks is not entirely clear, it was evident that EU supervised entities will no longer have access to the widest range of third country benchmarks.

The Commission’s consultation also requested views on a potential framework under which only certain third country benchmarks deemed “strategic” would remain subject to restrictions of use similar to the current rules. ESMA stated it was “somewhat in favour” of the proposal and that it would have been “totally in favour” if the level playing field between EU and third country administrators were ensured. ESMA also expressed the view that it should be the agency entrusted with supervision of “strategic” third country benchmarks.

ESMA are in agreement with the Commission that the creation of an EU ESG benchmark label would be a supporting tool against greenwashing and that sufficiently ambitious minimum standards for the methodology should be considered to offer reassurances as to the sustainability-related impact of such benchmarks.

ESMA suggested to the Commission that further analysis should be carried out to avoid unintended consequences if the legislation is amended. They offer the example that “to avoid excessive complexity of the regulatory framework, ESMA suggests reconsidering the several other categories of benchmarks currently identified by the BMR with the aim to simplify the regulatory framework.” Furthermore, ESMA stated that, in its view, the introduction of strategic benchmarks would render the two categories of “significant” and “non-significant” under the BMR unnecessary. However, as the “critical” benchmarks category is linked to additional BMR requirements, this category should be maintained.

The Commission’s consultation and the ESMA response reflect the fact that while BMR covers a wide range of benchmarks used by supervised entities in the EU, so far very few third country jurisdictions have followed a similar regulatory approach regarding the provision and use of benchmarks. When the Commission eventually proposes amendments to the third country regime in the BMR, it will be critical to strike a balance between minimizing the market impact of potentially removing the ability to permit EU institutions to use thousands of benchmarks administered in a third country, while not providing a competitive advantage to those third country administrators by exempting them from many or all of BMR requirements. The definition of a “strategic” benchmark will be a key part of this balancing act.

(The author wishes to thank trainee solicitor Ben Jacobs for his contributions to this article.)
