CADWALADER

CABINET NEWS

Research and commentary on regulatory and other financial services topics

Halfway Through: Financial Regulation Highlights

June 27, 2024

Table of Contents:

The U.S. Basel III Endgame Proposal: Update and Thoughts

June 27, 2024

By Christopher Horn
Partner | Financial Services

By Andrew Karp
Partner | Financial Regulation

On September 18, 2023, the U.S. Basel III Endgame proposal was **published in the Federal Register**. The comment period ended on January 16, 2024, with the banking regulators (the Federal Reserve, the OCC, and the FDIC) having received hundreds of **comments** on the proposal. Acknowledging the many concerns raised in the comment letters, Federal Reserve Chairman Jerome Powell indicated in his March 2024 Congressional testimony that "**there will be broad material changes to the proposal**." On June 24, **Bloomberg reported** that the Federal Reserve has "shown other US regulators a three-page document of possible changes to their bank-capital overhaul that would significantly lighten the load on Wall Street lenders."

At this writing, it remains unclear whether (or when) the banking regulators will adopt a final rule or, one hopes, issue a re-proposal. The banking regulators have been faced with the daunting task of analyzing the many technical and substantive concerns raised in the comment letters. Several other factors are contributing to the uncertainty surrounding the timing and nature of the banking regulators' next step, including:

- Joint Rulemaking. All three banking regulators must agree on any changes to the Basel III Endgame proposal. Reaching agreement on the "broad material changes" promised by Chairman Powell could take considerable time and effort, particularly given the differing perspectives of the three banking regulators.
- FDIC Leadership Transition. On May 20, 2024, FDIC Chairman Martin J. Gruenberg **announced** that he would step down from his position once a successor is confirmed. This transition could have the effect of causing a delay (*g.*, FDIC may be reluctant to act until a new chair is in place) or an acceleration (*e.g.*, FDIC may seek to issue a final rule before Chairman Gruenberg steps down) of the rulemaking process.
- CRA/November Elections. Congressional Review Act ("CRA") considerations could motivate the banking regulators to move quickly to adopt a final rule. Under the CRA, Congress can overturn a regulatory agency's final rule if a joint resolution of disapproval is (1) introduced within 60 legislative days following the date the final rule, (2) approved by both houses of Congress, and (3) signed by the President (or vetoed by the President, followed by a Congressional override). By moving quickly to adopt a final rule, the banking regulators could attempt to ensure that the 60-day CRA window closes before the new Congress is seated (and, perhaps, the new President takes office) following the November 2024 elections.
- Supreme Court Decision on Agency Rulemaking. The U.S. Supreme Court's decision in ***Loper Bright Enterprises v. Raimondo*** overturned the *Chevron* doctrine, thus limiting the degree to which courts must defer to regulatory agencies. Many of the comment letters assert that the Basel III Endgame proposal and related rulemaking process do not comply with requirements of the Administrative Procedure Act and existing caselaw construing such requirements. The *Loper* case opens the door to potential legal challenges of the final rule and could encourage the banking regulators to issue re-proposal that is narrower in scope.

Securitization Framework

As a reminder, the Basel III Endgame proposal includes significant changes to the mathematical model that assigns credit risk weights to securitization exposures. Both the existing "simplified supervisory formula approach" ("SSFA") and the proposed "securitization standardized approach" ("SEC-SA") incorporate a formula, referred to as

$$K_{SSFA}$$

and

$$K_{SEC\text{-}SA}$$

respectively, that calculates the average value of the marginal risk weighting function

$$K'(t) = e^{\left(-\frac{1}{pK_A}\right)(t-K_A)}$$

over the interval *t* = *A* to *t* = *D*. Under this function, *A* and *D* are the attachment and detachment points, respectively, of a securitization exposure, *p* is the supervisory calibration parameter (the p-factor), and K_A is the capital requirement of the underlying exposures, adjusted for defaults.

Of particular concern is the increase in the p-factor from 0.5 (under SSFA) to 1.0 (under the proposed SEC-SA). As the Structured Finance Association's ("SFA") **comment letter** explains, the increase in the p-factor from 0.5 to 1.0 effectively doubles the securitization capital surcharge and creates a host of anomalies. These points were emphasized by the SFA in a later meeting with the staffs of the banking regulators (pages 18-28 of the **meeting summary** contain helpful illustrations).

We note that p-factor value is a topic of concern not only in the U.S., but also on the UK and the EU. *See, e.g.*, **The UK's PRA Discusses Securitisation Capital Requirements and Basel 3.1**, by Alix Prentice, a partner in our London office.

Securitization market participants who are interested in the next stage of the Basel III Endgame rulemaking should consider joining SFA's **Basel III Task Force**, which is led by W. Scott Frame, the Chief Economist & Head of Policy at the SFA. Scott recently authored **De-Risking Banks through Synthetic Securitization and Credit-Linked Note Issuance**, which is an excellent overview of bank credit risk transfer ("CRT") transactions. CRT transactions would be significantly affected if the Basel III Endgame proposal is adopted in its current form.

We also bring to your attention the **Basel III Endgame Blog Series**, by Dr. Guowei Zhang and Dr. Peter Ryan of the Securities Industry and Financial Markets Association ("SIFMA"). Part X ("How the Basel III Endgame Could Impair Securitization Markets and Harm US Businesses and Consumers") is particularly insightful.

Federal Regulators Publish Final Rule on Automated Valuation Models and AI That Imposes Obligations on Secondary Market Issuers, Especially the GSEs

June 27, 2024

By Mercedes Kelley Tunstall
Partner | Financial Regulation

On June 6, 2024 federal regulators published **a final rule addressing Quality Control Standards for Automated Valuation Models**. This was a collaborative rulemaking effort that included regulators from the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve, the National Credit Union Administration, the Consumer Financial Protection Bureau ("CFPB") and the Federal Housing Finance Agency. The rule takes effect twelve months from the data of publication in the Federal Register, and as of the date of this Cabinet, the final rule has still not been published in the Federal Register. As the CFPB explains in a **blog post entitled "CFPB Approves Rule to Ensure Accuracy and Accountability in the Use of AI and Algorithms in Home Appraisals" regarding the final rule**, the new rule, which is largely consistent with the **proposed rule** published last year, "requires companies that use . . algorithmic appraisal tools to put safeguards into place to ensure a high level of confidence in [home] value estimates, protect against the manipulation of data, avoid conflicts of interest, and comply with applicable nondiscrimination laws."

Stemming from Dodd-Frank amendments to the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 ("FIRREA"), this new rule applies to "automated valuation models" ("AVMs") that are used to "determine the collateral worth of a mortgage secured by a consumer's principal dwelling." The scope of the rule covers both mortgage originators that use AVMs for credit decisions, but also secondary market issuers (i.e., "any party that creates, structures, or organizes a mortgage-backed securities transactions) who use AVMs to make certain determinations regarding securitizations, and the rule is focused upon ensuring that the AVMs used meet certain quality requirements. The secondary market issuer activity that is covered is called a "covered securitization determination", which is defined to mean "a determination regarding: (1) Whether to waive an appraisal requirement for a mortgage origination in connection with its potential sale or transfer to a secondary market issuer; or (2) Structuring, preparing disclosures for, or marketing initial offerings of mortgage-backed securitizations." The Federal Register commentary generally identified the GSEs as being subject to these requirements, but the requirements would apply to any secondary market issuer. Significantly, certain AVM uses are not covered by the rule, specifically when AVMs are used solely to review completed determinations and also when licensed appraisers use AVMs to prepare an appraisal. Note, however that non-licensed individuals who prepare evaluations of home value, but not appraisals, must ensure their AVMs meet the quality requirements of the rule.

In terms of the quality requirements, the final rule adopts what the regulators describe as "a flexible approach to implementing the quality control standards [that would] allow the implementation of the standards to evolve along with AVM technology and reduce compliance costs." This approach does not seek to foster uniformity in the AVM market. Instead, "[t]he quality control standards adopted are clear and simple" and are consistent with the "four quality control factors from the statute", but also include a fifth factor not in the statute, but implied, the regulators argue, by other laws, which is to ensure AVMs protect against discrimination. As such, mortgage originators and secondary market issuers using AVMs for a covered reason must "adopt and maintain policies, practices, procedures, and control systems" to ensure that the AVMs adhere to the following quality control standards: (1) That there is a high level of confidence in the estimates produced; (2) Protection against the manipulation of data; (3) Avoidance of conflicts of interest; (4) Required random sample testing and reviews; and (5) Compliance with applicable nondiscrimination laws.

On the technology side of things, the regulators note that some valuation products in the marketplace that do not "currently meet the definition of an AVM may meet that definition in the future" through the use of artificial intelligence, machine learning and other technologies. Accordingly, all valuation products generally (i.e., not just those that are technically AVMs) that are (1) automated; (2) a model, as defined by the **Interagency Supervisory Guidance on Model Risk Management**; and (3) designed to estimate the value of a consumer's principal dwelling collateralizing a mortgage, are subject to the quality control requirements.

Nota bene -- A quick aside on the use of the term "AI" by the CFPB (and by yours truly, at least in the title of this piece) in describing the algorithms that are used in typical AVMs – just because software uses algorithms does not necessarily mean that the software is "artificial intelligence" in the sense that is being marketed everywhere these days. The financial services industry has used algorithms for decades, for all sorts of purposes. It is important that folks

(and regulators) understand that just because algorithms are involved, that does not mean that they constitute “AI”, necessarily. Of course, do notice that the CFPB phrased the blog post title so that it suggests the rule addresses algorithms **and** AI, and not just AI, so presumably they know the difference.

The UK's Financial Conduct Charges Reality TV Stars With Illegal Financial Promotions

June 27, 2024

By Alix Prentice
Partner | Financial Regulation

The UK's Financial Conduct Authority ("FCA") has brought charges against several reality show participants for illegally issuing unauthorised financial promotions. These relate to an investment scheme that provided advice on buying and selling contracts for differences ("CFDs") without an authorisation to do so.

As a reminder, in 2018 the FCA imposed significant restrictions on firms offering CFDs and CFD-like options to retail customers. Having determined that CFDs are complex, leveraged derivatives, the FCA made its intervention in order to: limit leverage; require the closing out of a customer's position when funds fall to 50% of the required margin for open positions; provide protections such that a client cannot lose more than the total in their trading account; limit offers of inducements to trade; and require a standardised risk warning that tells potential customers of the percentage of retail accounts that make losses. These protections are on top of rules that require that financial promotions – which are broadly defined as any form of offer or inducement to engage in regulated financial activity – to be either issued or approved by an appropriately FCA-authorised firm.

In the case of this CFD scheme, the allegation is that the Instagram account @holly_fxtrends provided advice on dealing in CFDs without the requisite authorisation, and its owners paid several reality stars to act as 'finfluencers' and promote the Instagram account to their followers, thereby issuing unauthorised communications of financial promotions. The FCA has been concerned for some time over the role of social media to communicate financial promotions in a way that engenders consumer harm, and addressed this in **FG24/1: Finalised guidance on financial promotions on social media (fca.org.uk)** published in March 2024. While recognising that social media has an increasingly important role to play in marketing strategies for financial products, the Guidance is clear that a financial promotion issued through such channels is subject to the same requirement and restrictions as a promotion issued through more traditional media.

A plea and trial preparation hearing has been fixed for 11 July for all six defendants.

How FCA Guidance Aligns With Global Cyberattack Measures

June 27, 2024

Alix Prentice and Grace Ncube
Featured in *Law360*

CADWALADER

By March 31, 2025, U.K. firms regulated by the Financial Conduct Authority will be required to have conducted mapping and testing to ensure they remain within their impact tolerances for identified operational risks of cyberattacks for each important business service.

Ahead of this deadline, the FCA published a web page last month updating its guidance on operational resilience and providing further insights and expectations for firms to meet.

This article examines the guidance from the FCA and other global regulators on how firms can prepare for cyberattacks. It highlights the recurring themes presented by some of the most prominent regulatory authorities as well as areas that continue to be identified as under-provisioned.

Background The FCA has long been at the forefront of establishing comprehensive guidelines for operational resilience among financial institutions.

Recent initiatives include 2019's consultation paper on operational resilience and impact tolerances for important business services, which called on regulated firms to enhance their ability to withstand, respond to, and recover from disruptions.[1]

The consultation underscored themes that continue to resonate today, including the importance of identifying critical business services, setting impact tolerances, and conducting scenario testing to prepare for potential operational failures.

The goal was then, and is now, to ensure that firms could continue to deliver critical services even under adverse conditions, and thereby maintain the stability and integrity of the financial system.

Following that consultation, the FCA published a policy statement on building operational resilience in March 2021, outlining the rules that will apply to banks, building societies, Prudential Regulation Authority-designated investment firms, insurers and recognized investment exchanges.[2]

FCA Expectations

The FCA's updated web page provides detailed guidance based on firms' preparations for complying with the policy statement. The guidance sets out key priorities for firms to focus on.

- Identifying critical services: Regularly assess and justify the importance of business services;
- Impact tolerance: Establish clear boundaries for acceptable disruption levels;
- Mapping and third parties: Document and manage third-party relationships required for a firm to deliver each of its important business services;
- Scenario testing: Conduct rigorous testing to handle severe disruptions;
- Vulnerabilities and remediation: A firm's mapping and scenario testing must identify and address weak points that may put impact tolerances at risk;
- Response and recovery plans: Develop, test and refine disruption response plans;
- Governance and self-assessment: Ensure comprehensive board-approved assessments; and

- Embedding operational resilience: Embed resilience into corporate culture and risk management;
- Horizon scanning: Continuously monitor and update resilience strategies against emerging risks.[3]

The FCA's requirements highlight the importance of firms being able to anticipate, prevent, recover from and adapt to a wide range of operational disruptions.

This proactive stance is essential for maintaining the stability of the financial system and protecting consumers. Importantly, the guidance also sets out observations that the FCA has made on poor or incomplete practices — a form of a what-not-to-do guide.

For example, the FCA web page notes that some impact tolerances lack sufficient rationale for a firm's board to understand what parameters have been set and why.

Additionally, impact tolerances have been predominantly set as time-bound tolerances, and firms should consider using additional metrics such as customer types, transaction values and transaction criticality, as well as estimated losses, in order to truly anticipate how a significant disruption might play out.

International Perspectives

Globally, financial regulators are increasingly prioritizing operational resilience as essential to the health and continuity of financial systems. Notable international frameworks include those from the International Organization of Securities Commissions, or IOSCO, and the Swiss Financial Market Supervisory Authority, or FINMA.

IOSCO

On June 5, IOSCO published its final report on market outages, which addresses the critical need for improved preparedness and management of market outages.[4]

The report outlines five good practices aimed at enhancing resilience:

- Detailed outage plans: Establishing and publishing detailed outage plans to ensure that all stakeholders are aware of the procedures to follow in the event of a disruption;
- Comprehensive communication plans: Developing comprehensive communication plans to keep market participants informed during outages. This is essential for maintaining transparency and trust;
- Reopening protocols: Implementing protocols for the reopening of trading postoutage;
- Operating closing auctions: Operating closing auctions and establishing alternative closing prices to maintain market integrity; and
- Post-outage reviews: Conducting post-outage reviews to learn from each incident and improve resilience strategies, as well as adopting post-outage plans.

IOSCO's guidelines are designed to offer flexibility for adoption across various trading venues and jurisdictions. While not rules as such, this report again echoes the FCA's stance that operational resilience, and the ability to withstand increasingly focused and effective attacks and outages, remain a preeminent focus for all in the financial services industry.

FINMA

Switzerland's financial regulator, FINMA, has also been proactive in enforcing stringent operational resilience requirements. In its June updates, FINMA emphasizes the importance of cybersecurity measures, mandatory reporting of significant cyber incidents, and the necessity for firms to conduct regular stress tests to assess their operational resilience.[5]

The guidelines focus on:

- Cyber incident response plans: Firms must develop comprehensive cyber incident response plans, including clear roles and responsibilities for managing cyber
  incidents;
- Regular cybersecurity assessments: Firms must conduct regular cybersecurity assessments to identify and mitigate vulnerabilities;

- Board-level oversight: Firms must ensure that boards of directors have oversight of cybersecurity risks and resilience measures.

These measures are in line with FINMA's overarching goal of ensuring that financial institutions can withstand, recover from, and adapt to adverse conditions, thereby safeguarding the financial system's integrity.

Recent Cyberattack Examples

The necessity for operational resilience frameworks is underscored by recent cyberattacks on critical infrastructure, including financial institutions and healthcare systems. These incidents highlight the vulnerabilities that can be exploited, and the potentially significant impact of cyberattacks. What is also clear is that attacks are increasing in volume and sophistication, and that regulators are concerned that firms are not keeping up with challenges.

Conclusion

Despite extensive regulatory efforts, a common consensus among global regulators — including the FCA, IOSCO and FINMA — is that no firm can be entirely immune to cyberattacks or operational disruptions, hence no regime setting a zero-tolerance baseline.

However, there is clearly a prevailing frustration over an apparent lack of preparedness and insufficient investment in preventive measures by many firms.

Regulators continue to stress the importance of proactive strategies and robust resilience frameworks to mitigate the impact of such disruptions, while also observing a disappointing level of engagement by the industry.

A global theme over the years has been the necessity for firms to plan effectively, identify risks and ensure that senior management is regularly informed about potential threats and resilience measures.

Regulatory bodies have consistently emphasized that resilience is not just about compliance but involves ongoing investment in technology, training and robust governance. From the regulators' perspective, these measures are required to limit disruptions and are yet to be taken on board fully by firms.

Investing in operational resilience is not just about compliance; it is about safeguarding the financial system and protecting consumers. Regulators expect firms to move beyond minimum regulatory requirements and proactively enhance their resilience capabilities.

Recent cyberattacks illustrate the real-world implications of operational disruptions and the critical need for effective resilience strategies.

By adopting a proactive and comprehensive approach to operational resilience, firms can better protect themselves, their customers, and the broader financial system from the increasingly sophisticated and frequent threats posed by cyberattacks and other operational risks.

[1] https://www.fca.org.uk/publication/consultation/cp19-32.pdf.
[2] Policy statement 21/3: Building operational resilience: Feedback to CP19/32 (PS21/3).
[3] https://www.fca.org.uk/firms/operational-resilience/insights-observations.
[4] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD767.pdf.
[5] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=en&hash=A1A633E2246BE27B2020897E1A389049.