[DISCUSSION DRAFT]

119TH CONGRESS
2D SESSION

H. R. _____

To require the Board of Governors of the Federal Reserve System to evaluate the feasibility of real-time bank regulation by developing and testing open-source demonstration software that could be used by financial institutions and regulators, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. FOSTER introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Board of Governors of the Federal Reserve System to evaluate the feasibility of real-time bank regulation by developing and testing open-source demonstration software that could be used by financial institutions and regulators, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Real-Time Regulatory Study Act of 2026''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Real-time, 24/7 payment systems, tokenized deposits, and agentic artificial intelligence will deliver substantial convenience and efficiency to consumers and businesses.

(2) These technologies move money at machine speed, so deposit runs that once took days now take hours—

(A) on March 9, 2023, Silicon Valley Bank lost $42,000,000,000 of deposits in a single day, with more than $100,000,000,000 queued for withdrawal the following day;

(B) artificial intelligence-driven corporate treasury management and personal artificial intelligence financial assistants will further accelerate run dynamics; and

(C) both large and small financial institutions are susceptible to such runs.

(3) Halting a run in real time depends on immediate access to advances from central liquidity facilities, including the discount window of the Federal Reserve System, the Federal Home Loan Banks, and the Central Liquidity Facility of the National Credit Union Administration. This requires—

(A) real-time dashboards of capital, liquidity, and counterparty exposure that can be shared by institutions, regulators, and central liquidity facilities in times of stress;

(B) automated pre-positioning, valuation, and pledging of collateral; and

(C) immediate electronic transfer of advances.

(4) Bank management and regulation currently rely on overnight batch accounting, manual consolidation of incompatible data sets, quarterly self-computed and pre-aggregated reports, periodic examinations, and stress testing limited to a narrow set of economic scenarios and the largest institutions.

(5) Delays in supporting or resolving stressed institutions increase systemic contagion, shrink the pool of qualified bidders, and increase losses to guarantee funds and taxpayers; and such delays can be extended when available technology forces bank supervisors to resort to manual compilation of non-standardized data—

(A) the failure to promptly resolve Lehman Brothers was a substantial contributor to the financial crisis of 2008; and

(B) official reviews of the 2023 bank failures and the resolution framework of the FDIC, including report EVAL-25-02 of the Office of Inspector General of the Federal Deposit Insurance Corporation and report GAO-16-341 of the Government Accountability Office, document the challenges of compiling nonstandardized data that are often assembled manually over a compressed timeline.

(6) Rapid, transparent resolution of stressed depository institutions requires—

(A) automated generation of resolution data packages;

(B) full implementation of standardized data descriptors, like those intended by Congress under the Financial Data Transparency Act of 2022 (title LVIII of Public Law 117–263);

(C) pre-registration of qualified bidders, including entities other than insured depository institutions;

(D) cyber-secure bidder portals with standardized interfaces; and

(E) rapid, privacy-preserving transfer of customer data.

(7) Real-time fraud detection and anti-money-laundering reporting grow more important as cyber-enabled fraud accelerates—

(A) responding to this will require complex software that strikes a balance between privacy protection, reliable identity verification, broad coverage of asset classes, and real-time response; and

(B) a collaboratively developed reference implementation of controlled and appropriate data sharing will assist industry and Congress in striking that balance.

(8) Agentic artificial intelligence has greatly amplified cybersecurity threats. In particular—

(A) artificial intelligence tools are rapidly uncovering long-hidden vulnerabilities in widely used proprietary and open-source software components on which much of the internet and the financial system depend;

(B) attackers increasingly exploit such vulnerabilities before patches are available or widely deployed, and the window from patch publication to exploitation has shrunk from weeks to hours; and

(C) the government response to the disclosure of an artificial intelligence module with advanced cyber capabilities in April 2026 to large institutions, but not their smaller competitors, and the indecision regarding export controls for that module, highlight the need for clear governance of decisions about which software packages are to be prioritized when new cyber threats and capabilities emerge.

(9) Collaboratively maintained open-source core software packages, heavily used in the cloud infrastructure on which our financial system currently depends, when supported by enhanced collective maintenance and security built in from the start, are an effective strategy for dealing with these challenges by—

(A) eliminating duplication of effort in finding and patching the same cybersecurity flaw in multiple proprietary packages;

(B) clarifying the core software packages that are to be prioritized when new cyber threats emerge;

(C) simplifying the synchronized deployment of software patches; and

(D) allowing smaller institutions to benefit from the cybersecurity efforts and expertise of larger institutions.

(10) Realizing these benefits requires addressing the risks of shared software, in that—

(A) a single flaw can affect every user at once;

(B) critical components are best maintained by large, well-funded teams; and

(C) open-source banking software, if widely adopted, could create similar shared exposure, and therefore must be built with security from the start and supported by enhanced collective maintenance.

(11) Complex real-time software is increasingly out of reach for small and de novo institutions, and the resulting technology gap is a powerful barrier to new entrants and a driver of bank consolidation.

(12) Access to state-of-the-art, cybersecure, and regulatory-compliant real-time open-source banking software at nominal cost would significantly assist the survival of community financial institutions and innovative financial technology companies, in that—

(A) commercial software for real-time bank regulation is not widely available, especially to

smaller institutions, and commercial real-time core banking software has limited integration with regulatory data flows;

(B) the technology for real-time capital and liquidity dashboards has been developed for internal use by large bank holding companies and trading firms, frequently using open-source components;

(C) a core banking and regulation software package with a modular design with fully-specified interfaces will allow banks to run a mixture of standard open-source modules and premium commercial components, thereby providing opportunities for continued commercial innovation; and

(D) open-source regulatory software would increase transparency and predictability of regulator capabilities in times of crisis.

(13) A standardized open-source software package to automatically generate periodic regulatory reports would substantially reduce regulatory burdens and costs, especially for small market participants.

(14) An open-source reference implementation of software capable of providing real-time data on bank operations and regulatory compliance, using

synthetic data is an appropriate work product of a dedicated study, since—

(A) the Financial Data Transparency Act of 2022 directed the Federal financial regulators to adopt machine-readable data standards, and a reference implementation software implementing standardized metrics, terminology, and date schema is the natural next step; and

(B) the Federal Reserve has, since 2019, required its largest borrowers to report pledged loans in a standardized, machine-readable, loan-level format, and in September 2026 partially automated the maintenance of pledged-loan lists; extending that standardization to all depository institutions, to the Federal Home Loan Banks, and to real time is a natural next step.

SEC. 3. DEVELOPMENT OF DEMONSTRATION SOFTWARE.

(a) IN GENERAL.—The Board shall, in coordination with the designated entities, and after consultation with the consulting entities, develop, test, and make publicly available the following demonstration software modules:

(1) BANKING RECORDS AND OPERATIONS MODULE.—A module or modules that can be used by financial institutions to provide—

(A) a real-time double-entry ledger with real-time pledgeable-asset management, including management dashboards at the business-unit and consolidated bank holding company levels;

(B) interfaces to multiple payment rails, including instant, batch, wire, card rails, and other appropriate payment systems, as determined by the Board, with explicit representation of the settlement state of each obligation; and

(C) customer and counterparty portals; online customer onboarding with know-your-customer verification using mobile identification credentials consistent with standards of the National Institute of Standards and Technology; and open-banking customer data portability.

(2) REAL TIME REGULATORY DASHBOARDS.—A module that includes dashboards that may be used by regulators of depository institutions that provide current information about capital, available funds, incoming and outgoing payments, compliance with financial requirements, and financial risks involving other firms, including relevant information about an

institution's business units and affiliated companies, such as affiliated broker-dealers.

(3) REAL-TIME CENTRAL LIQUIDITY FACILITY SOFTWARE.—A module, or modules, that allows for access by financial institutions to the discount window of the Federal Reserve System, the Federal Home Loan Banks, and the Central Liquidity Facility of the National Credit Union Administration and supports—

(A) collateral pre-positioning, pledging, and advances, that interfaces to the securities settlement systems on which pledged collateral is held and transferred; and is compliant, to the extent possible, with the requirements of the Financial Data Transparency Act of 2022 and existing industry standards, and harmonized with the Automated Loan Deposit format prescribed by the Board and the collateral schedules of the Federal Home Loan Banks;

(B) internal liquidity management; and

(C) transparent, open-source valuation of pledgeable assets.

(4) PERIODIC REGULATORY REPORTING.—A module that allows for automated generation of regularly scheduled reports required to be compiled by

regulators of financial institutions, including the Consolidated Reports of Condition and Income of banks and the call reports of credit unions, the FR Y-15 Banking Organization Systemic Risk Report, Community Reinvestment Act reports, and other periodic reports determined by the designated entities.

(5) STRESS TESTING.—A module that can be run by individual financial institutions and by regulators, using historical and current data; allowing for the simulation of plausible stress scenarios, including nightly execution of a library of such scenarios that can identify a broad range of potential risks to the stability of a financial institution.

(6) REAL-TIME AML SCREENING AND SAR GENERATION.—A module that allows for—

(A) automated anti-money-laundering, suspicious-activity, and fraud screening and reporting;

(B) logging of manual decisions; and

(C) privacy-preserving data sharing among institutions, in accordance with applicable law.

(7) ARTIFICIAL INTELLIGENCE RISK MONITORING.—A module that has 1 or more nonbinding artificial intelligence advisory tools, trained on the

history and literature of bank failures and on historical supervisory data in accordance with section 2(g), to help financial institutions identify financial risks, operating on each institution's own records without disclosure to third parties.

(8) RESOLUTION DATA PACKAGE AND BIDDER PORTAL.—A module that allows for—

(A) organizing of records of deposits, loans, securities, qualified financial contracts, transactions with affiliated companies, positions and margin at each central counterparty of which the financial institution is a member, other obligations as of a specified time, and other information determined appropriate by the Federal Deposit Insurance Corporation or the National Credit Union Administration to resolve an institution put into receivership;

(B) checking the records described in subparagraph (A) against the financial institution's internal records, as appropriate; and

(C) securely sharing appropriate information with authorized regulators and potential purchasers in the event the financial institution is put into receivership.

(9) SYSTEM WIDE ORCHESTRATOR AND EVENT PACKAGE.—A module that allows financial institutions to simulate historical and hypothetical financial events, including the impact of the failure of a single counterparty or multiple counterparties to the financial institution, in which insolvency or a disruption to the counterparty's operations could negatively affect the safety and soundness of the financial institution, disruptions to the market for Treasury securities and repurchase agreements, cybersecurity failures, and other risks to the stability of a financial institution, with documentation on key assumptions and limitations of the module.

(b) ADDITIONAL MODULES.—The Board may develop and test additional demonstration software modules, as determined appropriate by the designated entities that would promote safety and soundness of the banking system, reduce regulatory reporting costs for financial institutions, or improve access to necessary real-time supervisory information.

(c) PRIVATE SECTOR INVOLVEMENT.—The Board shall, when developing and testing the demonstration software modules developed under subsection (a), seek technical contributions, donated components, and individual consultations from open-source industry consortia, stand-

ards bodies, financial institutions of all sizes, core processors and other third-party vendors, academic researchers, and policy researchers. The Board shall ensure that any donated component incorporated into a demonstration software module meets the requirements of subsection (d)(8).

(d) DEMONSTRATION SOFTWARE REQUIREMENTS.—Each demonstration software module developed under subsection (a) shall—

(1) be made publicly available as open-source software;

(2) include a clear description of how the module exchanges information with other relevant systems, in compliance with—

(A) applicable data standards under Federal law; and

(B) where the Board determines appropriate, relevant industry and consumer protection standards;

(3) be tested for accuracy and reliability using synthetic data, including a determination of whether users of a module can trace figures produced by the module to underlying records and calculations and deterministically reproduce the results produced using the same input data;

(4) facilitate appropriate controls over access to information, verification of authorized users, and records of access and changes;

(5) identify the source and timing of data inputted into such demonstration software, material assumptions, and known limitations of the demonstration software;

(6) be designed, to the extent practicable, to allow financial institutions to use individual capabilities of the demonstration software with their existing software and reporting systems;

(7) to the extent practicable, summarize real-time information in dashboards that can be viewed by the management of a financial institution and its primary regulator or central liquidity facility, as appropriate, to facilitate regulatory reporting and other information sharing between a financial institution and its primary regulator or central liquidity facility under existing law; and

(8) be developed with security of the module as an important consideration from the start of development, in accordance with recognized secure software development practices, including those published by the National Institute of Standards and Technology, and be subjected to an independent se-

curity review, including a review using artificial intelligence tools, before publication and periodically thereafter.

(e) DEMONSTRATION SOFTWARE DESIGN GOALS.—The Board shall seek to demonstrate that the demonstration software modules developed under subsection (a) individually and collectively achieve, to the extent practicable—

(1) modular boundaries, published interfaces and specifications, permitting operation with a mixture of open-source modules and compatible commercial components;

(2) deterministic reproducibility and complete event lineage, such that identical inputs reproduce every regulatory figure exactly and every dashboard figure is traceable to the originating ledger events;

(3) generation of resolution data packages, as of the moment that a financial institution is put into receivership by either the Federal Deposit Insurance Corporation or the National Credit Union Administration, as appropriate, that reconcile exactly to the ledger of the financial institution, including both settled and unsettled transactions;

(4) real-time controls appropriate to managing the orderly transition of a financial institution into receivership;

(5) nightly execution of a library of stress scenarios on the current financial condition of the financial institution using the demonstration software module; and

(6) alignment of interfaces and data schemas used by the demonstration software module with applicable data standards under Federal law and with existing industry data standards.

(f) FLEXIBILITY IN DESIGN.—In carrying out this section, the Board may—

(1) split or merge functions of demonstration software modules;

(2) adapt existing open-source software, including tools that work with existing commercial reporting software systems used by financial institutions; and

(3) select the intervals at which to update data used by the demonstration software modules developed under subsection (a) such that real-time information about a financial institution's financial condition may be prepared by the demonstration software modules.

(g) USE OF SYNTHETIC AND HISTORIC DATA.—When demonstrating the abilities of demonstration software modules developed under subsection (a) to achieve the requirements described in subsection (b) and the goals described in subsection (c), the Board may only use—

(1) synthetic data; or

(2) historical data, if—

(A) the use and publication of such data would not violate any Federal law;

(B) information identifying customers in such data has been removed or otherwise protected through appropriate anonymization; and

(C) any confidential supervisory information contained in the data has previously, lawfully been made public or is not less than 15 years old and is approved for disclosure by the Federal agency that owns such data, in accordance with applicable Federal law.

(h) LIMITED USE OF DEMONSTRATION SOFTWARE MODULES.—The demonstration software modules developed under subsection (a) may only be used in a test environment and may not access actual customer accounts, execute live financial transactions, submit actual regulatory filings, or take actual supervisory or resolution actions.

(i) MILESTONES.—The Board shall, when developing, testing and making publicly available demonstration software modules under subsection (a), seek to achieve the following milestones:

(1) Not later than 60 days after the date of enactment of this Act, the Board shall have made a public call for participation in the study and donations of relevant software components.

(2) Not later than 90 days after the date of the enactment of this Act, the Board shall have—

(A) identified and directed specific Federal agencies to take the lead in assisting the Board in developing each module described in subsection (a); and

(B) published preliminary interface documents.

(3) Not later than 180 days after the date of the enactment of this Act, the Board shall have published an initial framework for the development of each software module described in subsection (a) that describes the intended functionalities of each such module.

(4) Not later than 365 days after the date of the enactment of this Act, the Board shall have pub-

lished all of the demonstration software modules described in subsection (a) using synthetic data.

(5) Not later than 18 months after the date of the enactment of this Act, the Board shall have executed of a whole-system stress test using the demonstration software modules developed under subsection (a), using synthetic data based on the data schemas and standards chosen by the Board in the development of the demonstration software modules, including a scenario involving the exploitation of a vulnerability in a widely-shared software component.

(j) OPEN-SOURCE DEPENDENCIES.—The Board shall identify the open-source software components on which each of the demonstration software modules critically depend, assess the adequacy of their maintenance and security of such components, and coordinate with organizations focused on open-sourced software and other relevant entities to strengthen the maintenance and security of such components.

(k) VULNERABILITY COORDINATION.—The Board, in consultation with the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology, shall establish a process for the coordinated disclosure and remediation of vulnerabilities in the demonstration software modules developed, tested, and made

publicly available under this section and the open-sourced software components identified under subsection (j), which provides timely notice to financial institutions of all sizes.

SEC. 4. REPORTS TO THE CONGRESS.

(a) INTERIM REPORT.—Not later than 180 days after the date of enactment of this Act, the Board shall submit to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate a report describing the progress made by the Board in developing, testing, and making publicly available demonstration software modules under section 3, including published interface specifications, the status of each module being developed by the Board, an inventory of donated components, and a preliminary plan for the security and maintenance of the modules developed, tested, and made publicly available under this section.

(b) FINAL REPORT.—Not later than 2 years after the date of the enactment of this Act, the Board shall submit to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate a report that—

(1) describes each demonstration software module developed under section 3;

(2) with respect to each such module—

(A) explains the reasons for major design choices; and

(B) describes the results of testing, including whole-system tests conducted on synthetic data, and provides an explanation of any detected shortcomings or failures;

(3) assesses, based on the testing of the demonstration software modules developed under section 3, the feasibility of using open-source software to facilitate each function described in section 3(b) and section 3(4);

(4) assesses the timeliness, accuracy, completeness, and supervisory usefulness of the information produced by each demonstration software module developed under section 3, including appropriate update intervals and limitations arising from missing data, valuation methods, or assumptions;

(5) determines whether the use of specified software or technology providers meeting standards prescribed by the Board or the use of the modules by financial institutions could support a presumption of compliance or regulatory safe harbor for particular reporting requirements or other requirements, and the conditions, safeguards, and legal authority that would be necessary to allow for such

use, including for regulatory reporting and real-time screening for money laundering, fraud, and suspicious activities;

(6) assess whether real-time information about a financial institution's capital, available funds, payments, collateral, and financial obligations involving other financial institutions can improve supervision, risk management, and stability of the financial system;

(7) assess whether better information and software can improve access to central liquidity facilities and preparations for the orderly resolution of failing institutions;

(8) makes recommendations concerning the implementation of the Financial Data Transparency Act of 2022 as it pertains to increasing the availability, efficiency, utility, and accuracy of material supervisory information;

(9) includes a proposed plan for ensuring the ongoing security, maintenance, and updating of the open-source software modules developed under section 3 and the open-source software components on which they depend, by public agencies, private organizations, or a combination of such entities that addresses the vulnerabilities and risks associated with

reliance on open-source software, including the timely deployment of security updates by financial institutions and their service providers and sustainable funding for maintenance;

(10) assesses the costs and potential savings for small financial institutions, large financial institutions, community banks, credit unions, and newly established financial institutions that made use of the demonstration software modules developed under section 3 based on a review of—

(A) current reporting practices with use of financial institutions' existing software compared with potential use of the demonstration software, including staff time and costs for gathering, preparing, checking, correcting, and submitting information;

(B) estimated initial and continuing costs associated with using the demonstration software modules developed under section 3, including transferring data, connecting to existing systems, vendor fees, computing services, cybersecurity, testing modules, maintenance, and training;

(C) whether institutions could use individual capabilities of the demonstration soft-

ware modules without replacing their existing banking systems;

(D) any actual savings in software licensing, development, and maintenance that would be actualized by making use of the demonstration software modules associated with the shifting of costs to other services or providers; and

(E) whether more frequent reporting would offset any expected savings identified under subparagraph (D) or create duplicative obligations;

(11) assesses possible effects associated with the use, by financial institutions, of the demonstration software modules developed under section 3 on competition between financial institutions of different sizes, the establishment of new financial institutions, financial institution consolidation, and the concentration of cybersecurity risk from reliance by many financial institutions on common software;

(12) recommends privacy protections and access controls for information inputted or derived from use of a demonstration software module developed under section 3 used during ordinary operations, financial stress, and resolution, including information about pledged assets; and

(13) includes any recommended legislative or administrative actions from the Board based, distinguishing actions available under existing authority from those requiring additional authority.

(c) PUBLIC AVAILABILITY.—The Board shall make the reports required under this section publicly available, subject to applicable law protecting confidential or otherwise protected information.

SEC. 5. MISCELLANEOUS.

(a) AGREEMENTS AND DONATIONS.—Notwithstanding section 1342 of title 31, United States Code, the Board may, for the purposes of carrying out this Act—

(1) accept gifts of software, services, and details of personnel; and

(2) enter into cooperative research and development agreements.

(b) USE OF FEDERAL RESERVE BANKS.—The Board may carry out this Act, in whole or in part, through one or more Federal Reserve Banks.

(c) RULES OF CONSTRUCTION.—Nothing in this Act may be construed—

(1) to require any financial institution to adopt any demonstration software module developed under this Act;

(2) to attach any examination or supervisory consequence to participation or nonparticipation by a financial institution in the development or testing of demonstration software modules under section 3;

(3) to permit the use of real customer data in the development or testing of demonstration software modules under section 3, except as provided in section 3(g); or

(4) to limit any existing supervisory, enforcement, or rulemaking authority of any designated entity or consulting entity.

(d) FUNDING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, the Board shall carry out this Act using the surplus funds or operating income of the Federal Reserve System and at the discretion of the Board, the activities required under this Act may be integrated into the broader supervision-technology agenda of the Board.

(2) LIMITATION.—The total amount obligated or expended by the Board under this Act may not exceed the amount the Board determines necessary to carry out this Act.

SEC. 6. DEFINITIONS.

In this Act:

(1) BOARD.—The term ''Board'' means the Board of Governors of the Federal Reserve System.

(2) CONSULTING ENTITIES.—The term ''consulting entities'' means the Financial Stability Oversight Council, the Federal Financial Institutions Examination Council, the Conference of State Bank Supervisors, the Federal Home Loan Banks, the Commodity Futures Trading Commission, the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency, and financial market utilities designated under section 804 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

(3) CENTRAL LIQUIDITY FACILITY.—The term ''central liquidity facility'' means the discount window of the Federal Reserve System, a Federal Home Loan Bank, or the Central Liquidity Facility of the National Credit Union Administration.

(4) DEPOSITORY INSTITUTION.—The term ''depository institution'' has the meaning given the term in section 3 of the Federal Deposit Insurance Act.

(5) DESIGNATED ENTITIES.—The term ''designated entities'' means the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the National Credit Union Adminis-

tration, the Federal Housing Finance Agency, the Bureau of Consumer Financial Protection, the Securities and Exchange Commission, and the Department of the Treasury, including the Office of Financial Research and the Financial Crimes Enforcement Network.

(6) DASHBOARD.—The term ''dashboard'' means an electronic display or interface that presents, in a simplified and organized form, real-time information generated, processed, or made available by one or more modules under section 6 for use by authorized personnel of a financial institution or of a regulator, which may be summarized or aggregated to highlight the financial condition, liquidity, payment activity, exposures, risks, or compliance of the institution, and which is, as appropriate, traceable to the underlying records and calculations.

(7) FINANCIAL INSTITUTION.—The term ''financial institution'' means any insured depository institution (as such term is defined in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813)) and any insured credit union (as such term is defined in section 101 of the Federal Credit Union Act (12 U.S.C. 1752)).

(8) OPEN-SOURCE SOFTWARE.—The term ''open-source software'' means software whose source code is publicly available under a license meeting criteria established and published by the Board, that permits public use, inspection, modification, and redistribution, and that is actively maintained with a documented process for responding to security vulnerabilities.

(9) REAL-TIME.—The term ''real-time'' means updating or processing information as relevant events occur or information becomes available, within a rapid and documented interval appropriate to the information and its use, rather than relying solely on periodic reports.

(10) SYNTHETIC DATA.—The term ''synthetic data'' means data generated algorithmically and corresponding to no actual person or institution.