

[DISCUSSION DRAFT]

119TH CONGRESS
2D SESSION

H. R. _____

To require the Federal banking agencies to conduct a study on the use of advanced technologies in fraud detection and prevention, with particular attention to community financial institutions, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To require the Federal banking agencies to conduct a study on the use of advanced technologies in fraud detection and prevention, with particular attention to community financial institutions, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Bank Fraud Tech-
5 nology Advancement Act of 2026”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) ADVANCED FRAUD DETECTION TECH-
2 NOLOGY.—The term “advanced fraud detection tech-
3 nology” includes artificial intelligence, machine
4 learning, predictive analytics, behavioral biometrics,
5 network analytics, data fusion tools, distributed
6 ledger-based monitoring tools, blockchain tracing
7 tools, and other emerging technologies used to de-
8 tect, prevent, or mitigate financial fraud.

9 (2) ARTIFICIAL INTELLIGENCE.—The term “ar-
10 tificial intelligence” has the meaning given that term
11 in section 5002 of the National Artificial Intelligence
12 Initiative Act of 2020 (15 U.S.C. 9401).

13 (3) COMMUNITY FINANCIAL INSTITUTION.—The
14 term “community financial institution” means—

15 (A) an insured depository institution with
16 total consolidated assets of \$10,000,000,000 or
17 less; and

18 (B) a credit union with total assets of
19 \$10,000,000,000 or less.

20 (4) CREDIT UNION.—The term “credit union”
21 means a State credit union or Federal credit union,
22 as such terms are defined, respectively, in section
23 101 of the Federal Credit Union Act (12 U.S.C.
24 1752).

1 (5) FEDERAL BANKING AGENCY.—The term
2 “Federal banking agency”—

3 (A) has the meaning given such term in
4 section 3 of the Federal Deposit Insurance Act
5 (12 U.S.C. 1813); and

6 (B) means the National Credit Union Ad-
7 ministration.

8 (6) INSURED DEPOSITORY INSTITUTION.—The
9 term “insured depository institution” has the mean-
10 ing given such term in section 3 of the Federal De-
11 posit Insurance Act (12 U.S.C. 1813).

12 (7) MACHINE LEARNING.—The term “machine
13 learning” has the meaning given that term in section
14 5002 of the National Artificial Intelligence Initiative
15 Act of 2020 (15 U.S.C. 9401).

16 **SEC. 3. STUDY ON ADVANCED TECHNOLOGIES IN FRAUD**
17 **DETECTION AND PREVENTION.**

18 (a) IN GENERAL.—The Federal banking agencies, in
19 consultation with the Secretary of the Treasury, the Fi-
20 nancial Crimes Enforcement Network, the Federal Trade
21 Commission, and appropriate law enforcement agencies,
22 shall jointly conduct a comprehensive study on the use of
23 advanced fraud detection technology by insured depository
24 institutions and credit unions.

1 (b) REQUIRED ELEMENTS.—The study required
2 under subsection (a) shall evaluate the following:

3 (1) CURRENT USE AND EFFECTIVENESS.—The
4 current use and effectiveness of advanced fraud de-
5 tection technology, including—

6 (A) the extent to which insured depository
7 institutions and credit unions of varying asset
8 sizes deploy advanced fraud detection tech-
9 nology;

10 (B) measurable outcomes relating to fraud
11 reduction, loss mitigation, and consumer protec-
12 tion; and

13 (C) barriers to adoption, including cost,
14 vendor concentration, interoperability con-
15 straints, regulatory uncertainty, data access
16 limitations, and liability concerns.

17 (2) COMMUNITY FINANCIAL INSTITUTION AC-
18 CESS.—Community financial institution access to
19 advanced fraud detection technology, including—

20 (A) challenges faced by community finan-
21 cial institutions in accessing or deploying ad-
22 vanced fraud detection tools;

23 (B) whether economies of scale disadvan-
24 tage smaller community financial institutions

1 relative to large community financial institu-
2 tions;

3 (C) options to facilitate shared services,
4 utility models, managed-service providers, or
5 consortium-based fraud detection platforms;
6 and

7 (D) recommendations to ensure regulatory
8 guidance is appropriately tailored to avoid dis-
9 couraging adoption by smaller community fi-
10 nancial institutions.

11 (3) ARTIFICIAL INTELLIGENCE AND MACHINE
12 LEARNING.—Artificial intelligence and machine
13 learning, including—

14 (A) the use of artificial intelligence and
15 machine learning models, applications, and tools
16 in detecting fraud patterns, anomalies, syn-
17 thetic identity fraud, and real-time payment
18 fraud;

19 (B) governance frameworks used by in-
20 sured depository institutions and credit unions
21 to manage fraud model risk, explainability, bias,
22 and validation; and

23 (C) interactions between fraud detection
24 models and consumer protection laws, including

1 fair lending and unfair, deceptive, or abusive
2 acts or practices standards.

3 (4) INFORMATION SHARING AND PUBLIC-PRIV-
4 VATE PARTNERSHIPS.—Information sharing and
5 public-private partnerships, including—

6 (A) the effectiveness of existing informa-
7 tion-sharing frameworks, including section
8 314(b) of the USA PATRIOT Act (31 U.S.C.
9 5311 note);

10 (B) whether expanded public-private part-
11 nerships or centralized fraud utilities would en-
12 hance detection capabilities;

13 (C) the feasibility of a voluntary fraud
14 analytics consortium accessible to community fi-
15 nancial institutions; and

16 (D) privacy, data protection, and cyberse-
17 curity considerations associated with expanded
18 data sharing.

19 (5) PAYMENTS SYSTEM RISKS.—Payments sys-
20 tem risk, including—

21 (A) fraud risks associated with instant
22 payments, wire transfers, ACH transactions,
23 check fraud, and emerging payment channels;
24 and

1 (B) whether advanced analytics can reduce
2 fraud while preserving settlement finality and
3 payment system stability.

4 (6) REGULATORY AND SUPERVISORY CONSIDER-
5 ATIONS.—Regulatory and supervisory considerations,
6 including—

7 (A) whether existing supervisory expecta-
8 tions create unintended barriers to innovation;

9 (B) the need for interagency guidance, reg-
10 ulatory clarity, or safe harbors to support tech-
11 nology adoption; and

12 (C) opportunities to harmonize expecta-
13 tions across Federal banking agencies.

14 (c) REPORT AND RECOMMENDATIONS.—

15 (1) REPORT.—Not later than 18 months after
16 the date of enactment of this Act, the Federal bank-
17 ing agencies shall issue a report to the Committee
18 on Financial Services of the House of Representa-
19 tives and the Committee on Banking, Housing, and
20 Urban Affairs of the Senate containing all findings
21 and determinations made in carrying out the study
22 required under this section, and make such report
23 publicly available, except for classified or supervisory
24 information.

1 (2) RECOMMENDATIONS.—The report required
2 under paragraph (1) shall include legislative, regu-
3 latory, or supervisory recommendations which may
4 include—

5 (A) proposals to support shared fraud de-
6 tection utilities or consortium-based analytics
7 platforms;

8 (B) guidance or safe harbors to encourage
9 responsible artificial intelligence use in fraud
10 prevention;

11 (C) options to reduce vendor concentration
12 risk;

13 (D) pilot programs or regulatory sandboxes
14 tailored to community financial institutions;
15 and

16 (E) recommendations to strengthen public-
17 private information sharing consistent with pri-
18 vacy and civil liberties protections.

19 **SEC. 4. COMMUNITY BANK FRAUD TECHNOLOGY PILOT**
20 **PROGRAM.**

21 (a) IN GENERAL.—Not later than 1 year after sub-
22 mission of the study under section 3, the Federal banking
23 agencies may jointly establish a voluntary pilot program
24 to facilitate community financial institution access to ad-
25 vanced fraud detection tools.

1 (b) PROGRAM FEATURES.—The pilot program de-
2 scribed in subsection (a) may include—

3 (1) pooled procurement or shared services mod-
4 els;

5 (2) model validation assistance or technical sup-
6 port;

7 (3) standardized vendor risk management tem-
8 plates;

9 (4) regulatory clarity regarding model govern-
10 ance expectations; and

11 (5) collaboration with the Department of the
12 Treasury and law enforcement to provide
13 anonymized fraud typology data feeds.