upstate

REFERENCE DOCUMENT · COMMUNITY BANKS AND CREDIT UNIONS

AI in Community Banks and Credit Unions: Scenario Reference

Nine operating scenarios, the risks they create, recommended controls, and the governance sources behind them.

Version	September 2026
Sources current as of	September 2026
Audience	Community bank and credit union leadership
Status	General information; not legal advice

1. Introduction

1.1 Purpose

This document describes nine situations that community banks and credit unions commonly encounter as AI enters their software and daily work. For each situation it states the risk, the recommended controls, what good looks like, and the key sources behind it.

1.2 Audience

Chief executives, board members, and risk, compliance, lending, operations, and technology leaders at community banks and credit unions.

1.3 How to use this document

Select an AI tool the institution uses or is considering. Identify the relevant sections and review them with the people responsible for the tool, using its approval record and most recent review. Record gaps and assign follow-up owners. Sections 2 through 10 follow a fixed structure: Situation, Risk, Recommended controls, What good looks like, and Key sources. Appendix A lists every source with its link.

1.4 Scope and limitations

This document is general information, not legal advice. Applicability of any rule depends on the institution's charter, regulators, footprint, and activities; confirm obligations with counsel and the institution's regulators. Sources are current as of September 2026. Supervisory guidance is not binding on its own, but examiners use it to assess programs.

1.5 Contents

PART 1: INTRODUCING AI

2. Staff use of general-purpose AI tools

2.1 SITUATION

An employee identifies an AI writing assistant that could help draft customer emails. The institution has not stated which tools are permitted or which information may be entered into them.

2.2 RISK

Without stated rules, staff may use unapproved tools on their own, including with customer information, or abandon a useful tool. No owner is accountable for the decision. This is sometimes referred to as Shadow AI.

2.3 RECOMMENDED CONTROLS

1. Define which tools staff may use and which information may be entered into them.
2. Assign an owner to each AI system and agree with the board on the level of AI risk the institution will accept.
3. Keep approvals and reviews in one place within the existing risk program.

2.4 WHAT GOOD LOOKS LIKE

> A written AI program that sits inside enterprise risk management: an acceptable use policy for generative AI, a named owner for every AI system, a risk appetite the board has approved, regular board reporting, and clear rules on what data may go into AI tools.

2.5 KEY SOURCES

- CSBS AI Supervisory Framework V1.0
- NIST AI Risk Management Framework (AI 100-1) and Generative AI Profile (AI 600-1)
- FFIEC IT Handbook, AIO booklet, AI and machine learning
- SR 26-2 / OCC Bulletin 2026-13, Model Risk Management Fed + OCC
- NCUA AI resource page NCUA
- NYDFS Industry Letter: Cybersecurity Risks Arising from AI NYDFS

Links for every source are in Appendix A: References.

PART 1: INTRODUCING AI

3. AI features in existing vendor software

3.1 SITUATION

A software update to the fraud platform or customer-management system adds AI features. The institution did not purchase them separately, so they are not recorded in its AI inventory. The same applies to tools staff have started using on their own.

3.2 RISK

The institution cannot govern AI it does not know about. Vendor-embedded and staff-added tools can affect credit decisions, sensitive customer data, or fair treatment without review.

3.3 RECOMMENDED CONTROLS

1. Ask vendors which AI features are available, which are enabled, and what data they can access.
2. Record vendor features and staff-added tools in the inventory alongside systems the institution built.
3. Prioritize review of uses that affect credit, sensitive customer data, or fair treatment.

3.4 WHAT GOOD LOOKS LIKE

> One inventory that covers AI the institution built, AI embedded in vendor software, and tools staff adopted on their own. Every entry has a risk tier, and entries that touch consumer credit decisions, nonpublic customer information, or protected characteristics are flagged.

3.5 KEY SOURCES

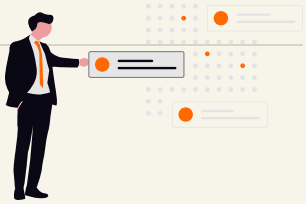
- CSBS AI Supervisory Framework V1.0 (Core Examiner Guide, Risk Tiering Worksheet)
- SR 26-2 / OCC Bulletin 2026-13, Model Risk Management `Fed + OCC`
- Proposed Third-Party Risk Management Guidance (2026) `All`
- NIST AI 100-1
- NYDFS Industry Letter: Cybersecurity Risks Arising from AI `NYDFS`

Links for every source are in Appendix A: References.

PART 1: INTRODUCING AI

4. Approval of an AI pilot

4.1 SITUATION



A team is ready to launch an AI pilot, and compliance is learning of the project for the first time. Questions about privacy and fair lending return the project to earlier stages.

4.2 RISK

An AI use goes live, or nearly does, before anyone has assessed its fair lending, consumer protection, or privacy exposure, and without agreed launch criteria.

4.3 RECOMMENDED CONTROLS

1. Designate a contact for proposed AI uses and identify who must review each one.
2. Match the legal, fairness, and privacy review to the proposed use.
3. Agree on launch criteria before testing begins. Include fair lending specialists for credit uses and advertising review for customer-facing claims.

4.4 WHAT GOOD LOOKS LIKE

> Every AI use passes a documented review before launch covering legal and consumer protection, fairness, and privacy. Go/no-go thresholds are written down before testing starts, and the use is reviewed again after any material change.

4.5 KEY SOURCES

- CSBS AI Supervisory Framework V1.0 (Core Examiner Guide)
- CFPB, Chatbots in Consumer Finance
- FTC v. Rite Aid Corporation; FTC Operation AI Comply
- Treasury, Artificial Intelligence in Financial Services
- NIST AI 100-1 and AI 600-1

Links for every source are in Appendix A: References.

PART 2: EVERYDAY USE

5. Reliance on vendor test results

5.1 SITUATION

A vendor provides test results for a model. The tests may have used data or customer populations that differ from the institution's own.

5.2 RISK

The institution relies on a vendor model that no one at the institution has tested against its intended use or can explain.

5.3 RECOMMENDED CONTROLS

1. Validate models before use, with testing proportionate to risk.
2. Review vendor evidence, test cases relevant to the intended use, and record limitations.
3. Include support, model changes, and ongoing review in vendor management.

5.4 WHAT GOOD LOOKS LIKE

> Models are validated before use, with depth scaled to risk. Vendor models meet the same standard through third-party due diligence and ongoing oversight. When a vendor will not share model details, the institution documents what it asked for, tests outcomes on its own data, strengthens monitoring and contract terms, and decides whether the residual risk is acceptable.

5.5 KEY SOURCES

- SR 26-2 and attachment Fed; FDIC FIL-15-2026 FDIC
- OCC Bulletin 2025-26, Model Risk Management for Community Banks OCC
- Interagency Guidance on Third-Party Relationships (2023) All
- Proposed Third-Party Risk Management Guidance (2026) All
- NCUA AI resource page NCUA

Links for every source are in Appendix A: References.

PART 2: EVERYDAY USE

6. Adverse action notices for AI-assisted credit decisions

6.1 SITUATION

A borrower is declined, and the notice does not explain what drove the decision. The lending team must trace the decision and provide the required reasons.

6.2 RISK

Use of AI does not change fair lending or notice obligations. Reasons that do not reflect the actual decision, or inputs that act as proxies for protected characteristics, create exposure under ECOA and Regulation B.

6.3 RECOMMENDED CONTROLS

1. Test for unfair outcomes and for inputs that may stand in for protected characteristics.
2. Confirm that the reasons in the notice reflect the actual decision.
3. Meet applicable Equal Credit Opportunity Act (ECOA) and Fair Credit Reporting Act (FCRA) notice requirements and retain supporting records.

6.4 WHAT GOOD LOOKS LIKE

> For any AI that touches credit: inputs are tested for proxies of protected characteristics, adverse action notices give the specific principal reasons for the decision, ECOA and FCRA notices go out on time, and supporting records are retained.

6.5 KEY SOURCES

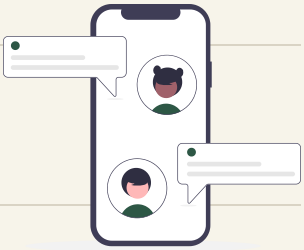
- Regulation B, 12 CFR 1002.9 (notifications) All
- Regulation B, 12 CFR 1002.12 (record retention) All
- Regulation B Official Interpretations (Supplement I) All
- CSBS AI Supervisory Framework V1.0

Links for every source are in Appendix A: References.

PART 2: EVERYDAY USE

7. Customer handoff from a chatbot

7.1 SITUATION



A chatbot gives a customer incorrect fee information. The customer must find someone who can resolve the issue and often repeats the conversation.

7.2 RISK

Chatbot errors about rates, fees, or terms are the institution's statements. A customer who cannot reach a person has no practical recourse.

7.3 RECOMMENDED CONTROLS

1. Check answers against approved rates, fees, and terms, and define where human review is required.
2. Require human approval before AI takes a consequential action.
3. Provide a clear path to staff, with the conversation history passed to them.

7.4 WHAT GOOD LOOKS LIKE

> People stay in the loop by design. Staff review generative AI output before relying on it, AI agents have a written map of what they may do and need approval before consequential actions, and customers always have a path to a person, including a way to challenge an AI-influenced decision.

7.5 KEY SOURCES

- CFPB, Chatbots in Consumer Finance
- CSBS AI Supervisory Framework V1.0
- FTC Act Section 5 (unfair or deceptive practices) All
- State and EU rules (Utah AI Policy Act, California ADMT regulations, EU AI Act) apply only where the institution operates.

Links for every source are in Appendix A: References.

PART 2: EVERYDAY USE

8. Monitoring AI after launch

8.1 SITUATION

A tool that passed testing begins to make more errors. Staff correct them individually, and no one records the pattern. A data change or vendor update may be the cause.

8.2 RISK

Model performance drifts without detection. No one has authority or written criteria to pause the tool, and no fallback has been tested.

8.3 RECOMMENDED CONTROLS

1. Track performance and give staff a way to report errors and near misses.
2. Set review triggers and name a person with authority to pause the tool.
3. Test the fallback process before it is needed to pause or retire the system.

8.4 WHAT GOOD LOOKS LIKE

> Every AI system in production has drift and performance metrics, a log of errors, near misses, and incidents, written criteria for pausing it, a channel for feedback and appeals, and a procedure for retiring it.

8.5 KEY SOURCES

- SR 26-2 and attachment Fed
- CSBS AI Supervisory Framework V1.0
- Proposed Third-Party Risk Management Guidance (2026) All
- FTC v. Rite Aid Corporation
- NIST AI 100-1 and AI 600-1

Links for every source are in Appendix A: References.

PART 3: SECURITY AND COMMUNICATIONS

9. AI in the information security program

9.1 SITUATION

A caller can use an AI-generated voice to impersonate an executive. Internally, an AI assistant can make overshared files easier to find. The two risks differ, but both belong in existing security planning.

9.2 RISK

AI-enabled impersonation and phishing, and exposure of overshared files through AI assistants. Incident reporting deadlines differ by regulator, and the point at which the reporting clock starts must be understood in advance.

9.3 RECOMMENDED CONTROLS

1. Verify unusual requests through a known contact, even when the voice sounds familiar.
2. Review file permissions before enabling an AI assistant, and use phishing-resistant sign-in protection.
3. Record each regulator's reporting requirements, including what starts the clock.

9.4 WHAT GOOD LOOKS LIKE

> AI threat scenarios are part of the security risk assessment. Phishing-resistant MFA is in place, exploited vulnerabilities are fixed quickly, inputs to AI tools are validated, and staff are trained on AI-driven social engineering. A current table lists each regulator's incident notice deadline. Before an AI assistant is enabled, file permissions are cleaned up.

9.5 KEY SOURCES

- NYDFS Industry Letter: Cybersecurity Risks Arising from AI NYDFS
- NYDFS 23 NYCRR Part 500 NYDFS
- Computer-Security Incident Notification rule (12 CFR 53, 225 subpart N, 304 subpart C) OCC, Fed, FDIC
- Treasury, Managing AI-Specific Cybersecurity Risks in the Financial Services Sector
- Credit union and state reporting timelines differ; confirm with the applicable regulator.

Links for every source are in Appendix A: References.

PART 3: SECURITY AND COMMUNICATIONS

10. Customer communications about AI

10.1 SITUATION

A draft announcement describes AI-assisted decisions as faster or fairer. The claims have not been substantiated, whether a person or an AI tool wrote the draft.

10.2 RISK

External claims about AI that the institution cannot support, and AI-drafted customer messages sent without accuracy review. Customers will reasonably expect service to match the description.

10.3 RECOMMENDED CONTROLS

1. Keep evidence for each external claim about what the AI does.
2. Review AI-drafted customer messages for accuracy before staff send them.
3. Explain limitations that affect what customers can expect.

10.4 WHAT GOOD LOOKS LIKE

> Every external claim about AI is substantiated, and every customer communication drafted with generative AI is reviewed before it goes out, through the existing advertising and compliance review.

10.5 KEY SOURCES

- FTC Operation AI Comply
- FTC Act Section 5 (unfair or deceptive practices) All

Links for every source are in Appendix A: References.

A. Appendix A: References

Governance documents, laws, and regulations cited in this document. Tags show who the source applies to: OCC (national banks and federal savings associations), Fed (state member banks), FDIC (state non-member banks), NYDFS (New York chartered institutions), NCUA (credit unions), All (every charter). Untagged sources are voluntary or apply through state supervisors.

Federal banking agencies

- SR 26-2, Revised Guidance on Model Risk Management (cover letter) Fed
  https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm
- SR 26-2 attachment, Revised Guidance on Model Risk Management Fed
  https://www.federalreserve.gov/supervisionreg/srletters/SR2602a1.pdf
- OCC Bulletin 2026-13, Model Risk Management: Revised Guidance OCC
  https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-13.html
- OCC Bulletin 2025-26, Model Risk Management: Clarification for Community Banks OCC
  https://www.occ.gov/news-issuances/bulletins/2025/bulletin-2025-26.html
- FDIC FIL-15-2026, Agencies Revise Interagency Model Risk Management Guidance FDIC
  https://www.fdic.gov/news/financial-institution-letters/2026/agencies-revise-interagency-model-risk-management-guidance
- Interagency Guidance on Third-Party Relationships: Risk Management (2023) All
  https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management
- Proposed Third-Party Risk Management Guidance (2026) All
  https://www.federalregister.gov/documents/2026/09/15/2026-18859/proposed-third-party-risk-management-guidance
- Computer-Security Incident Notification rule, OCC (12 CFR part 53) OCC
  https://www.ecfr.gov/current/title-12/part-53
- Computer-Security Incident Notification rule, Fed (12 CFR part 225, subpart N) Fed
  https://www.ecfr.gov/current/title-12/part-225/subpart-N
- Computer-Security Incident Notification rule, FDIC (12 CFR part 304, subpart C) FDIC
  https://www.ecfr.gov/current/title-12/part-304/subpart-C
- FFIEC IT Examination Handbook, AIO booklet: Artificial Intelligence and Machine Learning All
  https://ithandbook.ffiec.gov/it-booklets/architecture-infrastructure-and-operations/vii-evolving-technologies/viid-artificial-intelligence-and-machine-learning
- NCUA, Artificial Intelligence (AI) resource page NCUA
  https://ncua.gov/regulation-supervision/regulatory-compliance-resources/artificial-intelligence-ai

Consumer protection laws and regulations

- Regulation B (ECOA), 12 CFR 1002.9, Notifications All
  https://www.ecfr.gov/current/title-12/chapter-X/part-1002/section-1002.9
- Regulation B (ECOA), 12 CFR 1002.12, Record retention All
  https://www.ecfr.gov/current/title-12/chapter-X/part-1002/section-1002.12
- Regulation B, Official Interpretations (Supplement I to Part 1002) All
  https://www.ecfr.gov/current/title-12/chapter-X/part-1002/appendix-Supplement%20I%20to%20Part%201002
- CFPB, Chatbots in Consumer Finance All
  https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/
- FTC Act Section 5, 15 U.S.C. 45 (unfair or deceptive acts or practices) All
  https://www.law.cornell.edu/uscode/text/15/45
- FTC, Operation AI Comply: crackdown on deceptive AI claims (2024) All
  https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes
- FTC v. Rite Aid Corporation (stipulated order, 2024) All
  https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v

A. References (continued)

New York

- NYDFS 23 NYCRR Part 500, Cybersecurity Requirements NYDFS
  https://govt.westlaw.com/nycrr/Document/I60c644590d5f11e79781d30ba488e782
- NYDFS Industry Letter: Cybersecurity Risks Arising from AI and Strategies to Combat Related Risks (2024) NYDFS
  https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks
- NYDFS Industry Letter: Heightened Cybersecurity Risks Associated with Frontier AI Models (2026) NYDFS
  https://www.dfs.ny.gov/industry-guidance/industry-letters/20260521-heightened-cybersecurity-risks-assoc-with-frontier-ai-models

State supervisors

- CSBS AI Supervisory Framework V1.0, Core Examiner Guide
  https://www.csbs.org/sites/default/files/other-files/AI%20Supervisory%20Framework%20-%20Core%20Examiner%20Guide%20V1.0.pdf
- CSBS AI Supervisory Framework V1.0, Examiner Work Program
  https://www.csbs.org/sites/default/files/other-files/AI%20Supervisory%20Framework%20-%20Examiner%20Work%20Program%20V1.0.docx
- CSBS AI Supervisory Framework V1.0, Risk Tiering Worksheet
  https://www.csbs.org/sites/default/files/other-files/AI%20Supervisory%20Framework%20-%20Risk%20Tiering%20Worksheet%20V1.0.docx

Frameworks and reports (voluntary)

- NIST AI 100-1, AI Risk Management Framework 1.0
  https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
- NIST AI 600-1, Generative AI Profile
  https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
- NIST AI 100-2 E2025, Adversarial Machine Learning
  https://csrc.nist.gov/pubs/ai/100/2/e2025/final
- Treasury, Artificial Intelligence in Financial Services (2024)
  https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf
- Treasury, Managing AI-Specific Cybersecurity Risks in the Financial Services Sector
  https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf
- Cyber Risk Institute, FS AI RMF Risk and Control Matrix v1.0
  https://cyberriskinstitute.org/wp-content/uploads/2026/02/CRI-FS-AI-RMF-Risk-and-Control-Matrix_Full_v.1.0-2.xlsx

About Upstate AI

Ben Nichols, Founder & CEO

Ben helps community banks and credit unions move from AI curiosity to AI strategy. He works with executives and boards to find high-value uses, evaluate vendors without conflicts of interest, and build the internal capability to govern and scale AI responsibly. Before founding Upstate AI, Ben held leadership roles at the intersection of financial services and emerging technology. He also teaches at Syracuse University.

Ways to work together

Interactive AI workshop

A full day with leadership to cut through vendor claims, pressure-test use cases, and leave with a scored list of opportunities.

AI audit

A review of operations, governance, and vendors that ends in a prioritized roadmap with ROI estimates you can execute without us.

Part-time AI leadership

Ongoing guidance: vendor evaluation, board reporting, governance program build-out, and implementation support.

AI Execution

We manage your AI build from spec to launch: a clear technical plan, honest vendor evaluation, and a project manager who understands both the technology and your regulatory environment.

What this guide doesn't cover

- Commercial and small-business credit under Regulation B.
- BSA/AML and SAR decisions made with AI.
- Data rights and use terms in vendor contracts beyond model access.
- State law outside New York.
- A legal opinion for your institution. Confirm with counsel.

Contact	ben@up-state-ai.com
Book a session	up-state-ai.com/free-training.html
Online version	up-state-ai.com/ai-banking-guide