

Napkin Security Overview

Interim public overview for community banks and credit unions. This file restates the public security page at trynapkin.com/banking/security. It does not name certifications. A longer packet for internal review is requested from the security packet form. A counsel draft of that longer packet is pending.

Position

Napkin is an AI teller assistant for community banks and credit unions. It works during live conversations with members. This overview is the operational description of data handling.

Processing on Napkin's own machines

Inference and processing run on infrastructure Napkin operates. The institution's conversation data is not sent to a rented third-party model API for this work.

No third-party cloud AI APIs

Napkin does not call third-party cloud AI APIs to process these conversations.

Voice-only capture

The assistant hears the conversation. That is the capture surface.

Retention and deletion

The institution sets retention. Deletion follows that policy and can be requested. A default retention period is not published until counsel confirms it.

Access roles

Access is role-based. A teller sees prompts and task completions for their own conversations. A supervisor sees staff outputs for their branch. A compliance officer sees required-language outcomes and audit events for the institution. An admin sets retention, roles, and deletion.

Audit trail

The institution can see who accessed outputs, when, and what was changed. This is an institutional control over the record of the work. It is not a tool for watching staff.

Training

Institution data is not used to train models outside Napkin. Napkin does not use these conversations to train third-party models.

Certifications

None are claimed in this overview. A certification will be named only after it is approved.

Member disclosure

Institutions decide how to tell members that an AI teller assistant is present. Sample language on the website is sample language, not legal advice.