CheckCashing360 is management software used by licensed check-cashing businesses to run the counter, cash drawers, deposits, returned checks, compliance monitoring and reporting. This sheet summarizes how the business's data is stored and protected.

WHERE YOUR DATA IS STORED

- The database, sign-in service and file storage run on Supabase, in Amazon Web Services' US East (Ohio) region.
- The website and app are delivered by Netlify over HTTPS.
- Information is processed and stored in the United States.

ENCRYPTION

- All traffic uses HTTPS (TLS). The site sends a strict HSTS header, so browsers never connect without encryption.
- Stored data, including backups, is encrypted at rest with AES-256 by our database provider.
- Check account numbers are kept as a one-way fingerprint plus the last four digits, so duplicate checks are caught without storing the full number.
- Full ID numbers are kept in a separate, restricted record. Everyday staff screens show only the last four digits.
- Customer IDs, photos and check images are in private storage and open only through links that expire within minutes.

ACCESS CONTROLS

- Every business's records are separated inside the database with row-level security, so one business can never read another's data, even through the API.
- Roles — owner, manager, supervisor, cashier, compliance officer, auditor — with permissions limited to the locations each person works at.
- Two-step sign-in with an authenticator app. Owners can require it for their team.
- Automatic sign-out after a period of no activity, set by the owner.
- Our support team can enter a business's account only when the owner allows it, for a limited time, under their own name — never to move money — and every visit is shown to the owner.
- Restricted transactions need approval from someone with the right permission, and every check is screened for duplicates.
- Server keys and other secrets never reach the browser. Every request is checked on the server.

AUDIT TRAIL AND FINANCIAL RECORDS

- Every money movement, approval, reversal and access change is written to a permanent audit log that cannot be edited.
- Money is stored in whole cents and every transaction posts a balanced journal entry.
- Mistakes are corrected with recorded reversals and adjustments, never by deleting the original.
- Compliance tools (CTR worksheet, structuring alerts, OFAC screening) support your team's review; your compliance officer makes the decisions.

BACKUPS AND YOUR COPY OF THE DATA

- Our database provider backs up the whole database every day and keeps 7 days of daily backups.
- Separately, we make a full export of every table each week and keep the 12 most recent.
- Owners can download all of their records as CSV files at any time — including after cancelling.

AVAILABILITY

- The app runs on managed cloud hosting, and we monitor the database, scheduled jobs, emails and payments.
- App errors are reported to our team automatically.
- Planned maintenance and incidents are announced inside the app.
- We don't offer a formal uptime guarantee (SLA) today. If one matters to your bank, contact us.

SERVICE PROVIDERS

Supabase (on Amazon Web Services, US) — Database, sign-in and private file storage

Stripe — Subscription billing — we never see or store card numbers

Twilio — Text messages, only if the business turns them on

U.S. Census Bureau geocoder — Placing addresses on the map — store addresses, and customer street addresses only if the business turns on its customer map (no names or ID numbers)

Netlify — Website and app delivery

Resend — Email delivery

Mapbox — Drawing maps — receives the map area viewed, not customer data

OpenAI — Reading photos of IDs and checks, only if the business turns on photo scanning; issuer research (company details only, never customer data or account numbers). Not used to train models.