

SECURITY AND PRIVACY REPORT · FOR BUSINESS OWNERS

How we keep your customers' information safe.

What Keporia holds, where it is, who can see it, what we tested, and what we promise in writing. Written in plain words, with the proof attached.

THE ONE-PAGE VERSION

If you read nothing else, read this.

A loyalty card that lives in your customers' phones means you are trusting someone with your customers. Here is exactly what that trust involves.

1

thing we ask a customer for: their first name. No email, no phone, no birthday.

Toronto

where every record is stored. Our records never leave Canada.

72 h

the most we may take to tell you if anything is ever accessed without permission. It's in the contract.

A+

top grade on an independent security scan of both our website and the card system (proof on page 2).

What we hold about your customers

A first name, a member number, how many stamps they have, and a record of each stamp and reward with the time and the door. That is the whole list. Nothing that would let anyone contact, find or identify your customers outside your shop.

Who can see it

You, through your owner page. **Keporia** (one person), for support. **Nobody else.** Apple and Google deliver the card to the phone and see what's printed on it — the same as any card in a wallet. We never sell, rent or share it, and one shop's list is kept apart from every other shop's — we tested that, not just promised it.

Can a customer cheat the card?

No. The stamps don't live on the phone; they live in our database. The card is a signed picture of that record, and Apple and Google refuse to install a card that's been edited. A stamp can only be added at your counter or by your staff with a PIN. A screenshot of a "full" card gets nobody a free pizza.

What we tested

In September 2026 we ran a penetration test on the live system — we tried to break in, to read one shop's customers from another shop, to guess staff PINs, and to overload the server. Nothing let an outsider read or change anyone's data. One weak spot (a way to make the server work hard) was found and fixed the same day. Details and proof on pages 3–4.

What we promise in writing

- Your customer list is **yours**. You can have a copy any time, free, within ten business days.
- If a customer asks to be forgotten, we erase them — normally the same day.
- If anything is ever accessed without permission, you hear from us within 72 hours.
- If you leave, you take your list and your card design with you.

What we do *not* claim

We have not yet had an outside firm test us (planned once we have about ten clients). We have no SOC 2 or ISO certificate — no café or pizza shop should pay for one. Keporia is one operator. We would rather tell you that than let you find out.

PROOF 1 · INDEPENDENT SCAN

Top grade from an outside checker.

securityheaders.com is a free public tool run by Snyk, a security company. It checks how well a website protects the browsers of the people who visit it. It is independent of us, and you can run it yourself in ten seconds: go to securityheaders.com and type `keporia.ca`. Both of our sites were scanned on 7 September 2026. A+ is the highest grade it gives.

Security Report Summary



Site: <https://keporia.ca/>
IP Address: 75.2.60.5
Report Time: 07 Sep 2026 00:03:44 UTC
Headers: ✔ Content-Security-Policy ✔ Permissions-Policy ✔ Referrer-Policy ✔ Strict-Transport-Security
✔ X-Content-Type-Options ✔ X-Frame-Options
Advanced: Wow, amazing grade! Perform a deeper security analysis of your website and APIs: [Try Now](#)

Our website, keporia.ca — A+, all six protections present. Scanned 07 Sep 2026 00:03 UTC.

Security Report Summary



Site: <https://card.keporia.ca/j/keporia-demo>
IP Address: 66.241.125.132
Report Time: 07 Sep 2026 00:04:01 UTC
Headers: ✔ Strict-Transport-Security ✔ Content-Security-Policy ✔ X-Frame-Options ✔ X-Content-Type-Options
✔ Referrer-Policy ✔ Permissions-Policy
Advanced: Wow, amazing grade! Perform a deeper security analysis of your website and APIs: [Try Now](#)

The card system your customers use, card.keporia.ca — A+, all six protections present. Scanned 07 Sep 2026 00:04 UTC.

What those six green boxes mean, in plain words

Protection	What it does for your customers
Strict-Transport-Security	The browser will only ever talk to us over an encrypted connection. No "http://" fallback.
Content-Security-Policy	Only code we wrote can run on the page. No outside scripts, no trackers, no ad networks — nothing sneaks in.
X-Frame-Options	Our pages can't be hidden inside someone else's website to trick a customer into clicking.
X-Content-Type-Options	The browser can't be fooled into treating a file as something it isn't.
Referrer-Policy	When a customer leaves our page, we don't hand the next site the address they came from.
Permissions-Policy	Our pages may not use the camera, microphone, location or payment features — except the staff counter page, which scans cards.

Also true, and checkable in any browser: keporia.ca loads nothing from any third party — not even fonts — and sets no cookies. Nobody who visits it is tracked.

PROOF 2 · PENETRATION TEST, 6 SEPTEMBER 2026

We tried to break it. Here's what happened.

A **penetration test** is when you attack your own system the way a criminal would, to find the holes before they do. Ours was done in two independent passes on the same day, on the live system, and every finding was fixed and re-tested before the day was out.

What we tried

The attack	Result
Open every one of the system's 86 "doors" (web addresses) without a key	Blocked. Every door that touches data demands a key: a secret, a PIN, a token or Apple's own pass credential.
Read one shop's customer list while holding another shop's key	Blocked. Every lookup is fenced to the shop it belongs to. A card from another shop is "not from this shop."
Guess a staff PIN by trying thousands of combinations	Blocked. Five wrong tries locks that address out for five minutes — and see the next page for how we proved the lock can't be dodged.
Forge a customer's identity to see or redeem their card	Blocked. Identity is a long random token, never the member number printed on the card.
Edit a card on the phone to add stamps	Impossible by design. The card is digitally signed; a changed card won't install. Stamps live in the database, not on the phone.
Trick the server into showing files, running commands or revealing errors	Blocked. Every input is checked; errors show nothing about the inside of the system.
Redeem the same reward twice by clicking fast	Blocked. The database refuses the second one.
Make the server so busy it stops serving real customers	Found, then fixed. See below.

The one thing we found — and the fix, with numbers

One public image on our own business-card page was being redrawn from scratch every time anyone asked for it. We measured it on the live server: **5.8 seconds of work per request**. A dozen requests at once would have made the whole system slow for everyone. No data was at risk — but "the card wouldn't load at the counter" is a real problem for a shop.

Fixed the same evening. The image is now drawn once and remembered. Measured again after the fix: **0.11 seconds**. Two smaller cases of the same shape were fixed at the same time, and a limit was added so no single internet address can ask for unlimited cards.

Also added because of the test

A one-click "erase this customer" button. Canadian privacy law gives every customer the right to ask a business to delete them. Before the test there was no way to do that for a single person. Now there is: their record, their visit history and their card registrations are gone in one action, normally the same day you ask. That's a promise you can make to your customers.

PROOF 3 · WE TESTED THE LOCK, NOT JUST THE DOOR

Why the PIN lock can't be dodged.

Every lockout in the system — wrong PINs, wrong passwords, too many sign-ups — counts by the internet address the attempts come from. The obvious trick is to lie about your address so each guess looks like it came from somewhere new. We didn't assume that was impossible; we tried it.

The test: twelve wrong sign-in attempts against a demo shop's owner page, each one pretending to come from a *different* address, using three different ways of lying about it.

What a broken system would show: twelve "wrong password" answers and no lock — every guess treated as a fresh start.

What ours showed: 401 401 401 401 401 401 401 401 401 401 429 429 — ten "wrong password", then **locked out** on the eleventh, exactly as designed. The lies about the address were ignored, because our hosting provider stamps the true address on every request before it reaches us, and a visitor cannot overwrite it.

The same lock protects the staff PIN at your counter: five wrong tries, five minutes out. A six-digit PIN has a million combinations; at five tries per five minutes an attacker would need, on average, about a year — from a single address, with every other defence switched off.

How we keep it this way

Habit	What it means
Automatic tests before every change	Every time the system is updated, 299 checks run first — including the attacks above. If any check fails, the update does not go live. This has already stopped a bad update once.
Nothing secret in the code	The keys that sign your cards live in a locked store at the hosting provider, never in the code, never on a laptop. When one set of keys was exposed by accident in September, new keys were generated within minutes, the system was moved to them the same evening, and Apple was asked to revoke the old ones.
Backups every day, checked every week	A copy of the database is taken daily. Every Monday an automatic check confirms the newest copy is under two days old and emails us if not.
Two-factor sign-in everywhere	The accounts that could change the system — the code host, the server host, Apple — require a second factor to sign in.
Independent re-checks	Every finding in this report was verified by a second, independent review before it was written down. The first review's "we think it's safe" became the second review's "we proved it".

PRIVACY LAW · WHAT IT MEANS FOR YOU

Your customers' rights, already handled.

Under Canada's privacy law (PIPEDA) you are the business responsible for your customers' information, and Keporia works for you under a written agreement. Here is how each obligation is covered, so you never have to say "I'm not sure" to a customer.

A customer asks...	Your answer
"What do you have on me?"	"Your first name, your member number and your stamps. That's it." (You can show them on your owner page.)
"Where is it kept?"	"On servers in Toronto. It never leaves Canada."
"Who else sees it?"	"Nobody. It isn't sold or shared. Apple or Google show you your own card; that's all."
"Do you track where I am?"	"No. Your phone decides on its own whether to show the card near the shop. We never receive your location."
"I don't want the offers."	"Turn off notifications for the card in your phone's Wallet settings — or just delete the card."
"Delete me."	"Done — give me the number on your card." (One click on our side; normally the same day.)
"Is it safe?"	Hand them this report, or point them to keporia.ca/privacy.html — written for people, not lawyers.

What consent looks like

When a customer joins, the sign-up page shows plain wording. Agreeing to *offers* through the card is a separate, optional tick — the card works without it. We record the time and the exact words they saw, which is what Canada's anti-spam law asks for. We send no email and no text messages, ever; the only way to reach a customer is a message shown by the card itself, which they can switch off.

Published, public, dated

Our privacy policy, cookie statement, terms, refund policy and accessibility statement are all live at keporia.ca, linked from every page, each with a "last updated" date. Nothing in them says more than the system actually does.

If you're a franchisee

Your brand's logo and colours go on the card, so your franchisor may need to approve. That permission is yours to obtain, and we'll help you write the ask — we won't launch a card to the public without it. Everything in this report can be forwarded to a head-office IT or marketing team; the technical detail they'll want is on the last page.

APPENDIX · FOR THE IT OR HEAD-OFFICE READER

The technical summary.

Hosting. Application on Fly.io, region YYZ (Toronto). Single application instance, multi-tenant with query-level isolation; SQLite on an encrypted persistent volume; daily snapshots, weekly automated freshness check. Website on Netlify (static, no server code). Custom domains, HTTPS enforced, HSTS one year.

Transport and headers. TLS on every endpoint. CSP `default-src 'self'; script-src 'self'` — no inline script, no third-party script; `frame-ancestors 'none'`; nosniff; strict Referrer-Policy; Permissions-Policy denying camera/mic/geo/payment except the counter page (camera). Website loads zero external resources; fonts self-hosted. securityheaders.com A+ on both hosts (7 Sep 2026).

Data collected. Customer: first name, consent flag with timestamp and wording, referral link. System-generated: member number, balance, scan log (kind, delta, time, location id), Apple pass authentication token, device registration id and push token, Google Wallet object. No email, phone, DOB, payment or location data. Merchant: business details, staff PIN (per site), counter secret, owner token — all compared in constant time.

Authentication and authorisation. Admin API: bearer token, 503 if unconfigured, lockout after 20 failures/15 min per IP. Owner dashboard: per-merchant key, httponly/secure/samesite cookie, 30-day expiry, lockout after 10 failures. Staff: 6-digit PIN per site, lockout after 5 failures/5 min per IP+merchant. Customer identity: random 24-char token cookie per merchant, never the member number. Apple web service: per-pass authentication token, pass-type enforced on every call. Tenant isolation enforced at the query layer on every externally-supplied identifier; verified by route-level tests.

Rate limits (persisted, survive deploys). Enrolment 30/IP/hour; pass download 60/serial/10 min and 200/IP/10

min; self-stamp 1 per 90 min and 2/day; campaign 1 per merchant per 20 h; welcome portal 20/IP/hour. Request body capped at 64 KB (13 MB on admin upload). IP source is `Fly-Client-IP`, set by the edge and verified non-spoofable (test on page 4).

Pass integrity. Apple passes signed with a Pass Type ID certificate per client (one certificate per organisation), private keys held only in Fly's secret store, written to a 0600 file at boot. Compromised key material (Sep 2026) rotated within the hour; revocation requested from Apple (case 102955131196).

Change control. Push to main → 299 route-level tests + container smoke test → deploy → live health check. Dependencies pinned; weekly pip-audit and bandit scan; base image pinned by digest; container runs as a non-root service user. No public API documentation surface.

Privacy operations. Per-customer erasure (member, scans, passes, registrations; referral link nulled; Google object expired) — admin-gated, tenancy-checked, confirm-guarded, logged by member id only. Full-list CSV export on request within 10 business days. Breach notification to affected clients within 72 h; to the OPC where PIPEDA requires.

Testing. Internal penetration test 6 Sep 2026 (white-box review of all 86 routes plus live black-box probing, two independent passes). Findings: 1 medium (unauthenticated expensive render → memoised), 2 low/medium (same class), 1 low (error handling), 1 compliance gap (no per-customer erasure). All closed and re-verified same day. Full report available on request.

Known limitations, stated. No third-party penetration test yet (planned at ~10 clients). No SOC 2 / ISO 27001. Single machine, single operator. Backup restore not yet rehearsed (scheduled). Android geofence display is at Google's discretion and is not promised.

Keporia · Md Abid Hasan · St. John's, Newfoundland and Labrador · abid@keporia.ca · 709-660-9874 · keporia.ca
This report describes the system as it stood on 6–7 September 2026. It is a statement of fact about our own systems, not legal advice.