

Product Requirements Document (PRD)

Project Name Northern Legacy E-Commerce Portal

Version 1.0

Status Approved for Development

Date February 14, 2026

Author Greg Farrel, Lead Full-Stack Engineer

Stakeholders: Excelsior Genetics (Parent), Northern Legacy (Retail DBA)

1. Executive Summary

Northern Legacy is a licensed-pending microbusiness dispensing cannabis products in the 1000 Islands region in Upstate NY. This platform acts as a custom, vertically integrated regulatory gatekeeper, enabling compliant ordering for both Mainland (Land) and Maritime (Water) delivery.

The system must handle the extreme geographic complexity of the St. Lawrence River border region, enforcing a 30-mile "Hard Limit" radius and verifying that delivery coordinates remain strictly within U.S. sovereign waters/territory, independent of IP-address fluctuations common in border zones.

2. Technical Architecture

- **Frontend:** React.js (Vite), Tailwind CSS
 - **Backend:** Node.js, Express.js
 - **Database:** MongoDB (Mongoose)
 - **Geolocation:** Google Maps API + Plus Codes (for unaddressable island/dock locations)
 - **Identity Verification:** Persona/Jumio Sandbox (Digital) + Driver-App Scan (Physical)
-

3. Functional Requirements

3.1 Authentication & Compliance (The "Gatekeeper")

3.1.1 Age Gating: Mandatory 21+ splash modal upon initial application load to ensure immediate regulatory adherence.

3.1.2 Digital Identity Verification: Integration with a SOC-2 compliant third-party IDV (Identity Verification) provider (e.g., Persona or Jumio Sandbox).

- **System Logic:** The onboarding flow requires Optical Character Recognition (OCR) of a valid government-issued document (Passport, Driver's License, or State ID) combined with a Biometric Liveness Check (an active selfie). This ensures the user is a real, present human and prevents spoofing via static photos or stolen data.
- **Status Tracking and Webhooks:** The verification process operates asynchronously. The user profile field "isVerified" remains False until the backend receives a secure, encrypted webhook callback from the IDV provider confirming a verified match.
- **Exception Handling:** If the automated system flags the ID for minor discrepancies (e.g., camera glare or a recent name change), the status updates to "Pending Admin Review" allowing Northern Legacy management to manually verify the account without forcing the user to start over.

3.1.3 Physical Verification & The Handoff Token (Driver Protocol)

- To ensure strict regulatory compliance and prevent unauthorized handoffs, the system utilizes a closed-loop, dual-verification process at the physical point of delivery.
- **Handoff Token Generation:** Upon successful advance payment and route scheduling, the backend generates a secure, time-sensitive QR code (The Handoff Token). This code is cryptographically tied to that specific transaction ID and verified User ID.
- **Omnichannel Token Distribution:** To guarantee the customer has easy access to their token regardless of cellular service on the river, it is distributed across three touchpoints:
 - **Customer Profile:** Displayed prominently within the "Active Orders" tab of the user's Northern Legacy web application dashboard.
 - **Email Notifications:** Embedded directly into the initial order confirmation receipt and the automated "Your Order is Arriving" emails.
 - **Driver Manifest:** Synchronized to the specific order profile within the driver's routing application.

- **The Delivery Scan Protocol:** At the physical drop-off location (dock or door), the driver must use their application to complete two mandatory steps before releasing the product:
 - 1. Token Scan:** The driver scans the customer's QR Handoff Token. This confirms the customer possesses the device/email associated with the purchasing account.
 - 2. ID Verification:** The driver physically inspects the recipient's government-issued ID to ensure the person standing in front of them exactly matches the verified profile that placed the order.
- **Compliance Lock:** The backend will permanently block the driver from marking the order as "Completed" unless the QR token is successfully scanned and logged alongside a GPS-stamped coordinate confirming they are at the correct delivery location.

3.2 Border-Zone Geofencing & Anti-Spoofing

3.2.1 The Delivery Radius Logic:

- **Land Delivery:** Advertised radius of 25 miles (user-facing marketing), with a hard enforcement backend limit of 30 miles based on Haversine distance calculations.
- **Water Delivery:** The maritime delivery radius restriction will be determined at a later date following a comprehensive review of water delivery logistics.

3.2.2 Device-Level GPS Enforcement:

- **Logic: System** ignores IP Geolocation in favor of high-accuracy HTML5 navigator.geolocation to prevent border-town tower jumping.
- **Boundary Check:** Backend uses Google Maps Reverse Geocoding to ensure coordinates strictly resolve to country: US and state: NY.
- **Fail State:** If coordinates land in Canadian waters or mainland (regardless of the delivery radius), the transaction is immediately blocked and the user is notified of the regulatory restriction.

3.2.3 VPN/Proxy Detection:

- Backend will flag orders originating from known VPN exit nodes. If a VPN is detected, the user is blocked from entering the checkout flow until they disable the spoofing tool, ensuring true location verification.

3.3 Maritime & Land Logistics Scheduling

3.3.1 Delivery Route Selection: Users must define their terrain type at the start of checkout:

- **Type A (Land):** Standard street address. Selectable on Mondays, Wednesdays, and Fridays (Available year-round).
- **Type B (Water):** Island or dock delivery. Selectable on Thursdays, Fridays, and Saturdays (Seasonal Restriction: Active only from Memorial Day through Labor Day).

3.3.2 Seasonal UI Enforcement: Water delivery will only be available during the warm weather months

- **Logic:** The system backend must check the current date against the active seasonal window.
- **Action:** If the current date falls outside the Memorial Day to Labor Day window, the "Water Delivery" option is grayed out and disabled in the checkout flow.
- **User Feedback:** A tooltip or alert must display: "Water delivery is currently closed for the season due to weather conditions. Please select Land Delivery or In-Store Pickup."

3.3.3 Non-Addressable Locations (Plus Codes): For Water deliveries without a standard Google address, the UI presents an interactive Map Picker.

- **Implementation:** The user drops a pin. The application converts the pin's latitude and longitude into a Google Plus Code (e.g., 87G8MPG2+V3).
- **Benefit:** This Plus Code is saved as the official "Address" and passed directly to the driver's manifest for precise 3-meter accuracy maritime navigation.

3.4 Product Catalog & Compliance Limits

3.4.1 Inventory Sync: Real-time, bi-directional updates from the MongoDB backend to the frontend UI to prevent overselling during high-volume river events.

3.4.2 NYS Possession Monitor: The cart must prevent any user from exceeding the legally mandated daily possession limit for flower or concentrates. This requires dynamic weight calculation in the cart that disables the checkout button if limits are breached.

3.4.3 Dynamic Scarcity Indicators: The UI will dynamically display low-stock warnings (e.g., "Only 3 ounces remaining!") when a product's available inventory drops below a pre-defined backend threshold to drive urgency.

3.4.4 Admin Promotional Flags: Admins can manually tag specific inventory items via the dashboard with an "isLimitedRelease" or "isExclusive" boolean flag. These items will render in the customer UI with a prominent "Limited Time Availability" badge to highlight special drops.

3.5 Checkout & Payment Processing

3.5.1 Delivery Orders (Pre-Payment Mandatory):

- **Logic:** All delivery orders (both Land and Water) require full payment in advance via a compliant ACH/Digital PIN Debit gateway.
- **Enforcement:** The system must explicitly disable any "Cash on Delivery" or "Pay Later" options when a delivery terrain is selected to ensure driver safety and streamline dockside handoffs.

3.5.2 In-Store Pickup (Cash Reservations) & The 24-Hour Hold:

- **Logic:** Users selecting "In-Store Pickup" may bypass advance digital payment and select "Pay in Store" (Cash or Terminal).
- **Strategic Purpose:** This feature allows customers to secure high-demand, low-inventory, or exclusive items immediately upon receiving marketing notifications.
- **The 24-Hour Hold Rule:** The system will instantly deduct the reserved items from live inventory upon checkout. A backend cron job will continuously monitor the order timestamp; if the order is not marked "Completed" by an admin within 24 hours, it is automatically Cancelled and the products are immediately restored to the public inventory pool.

3.5.3 Automated Refund Processing:

- **Logic:** If a pre-paid delivery order is marked Cancelled (either manually by an Admin or automatically via the 24-Hour Hold cron job), the system must automatically fire a webhook to the ACH payment gateway to reverse the charge.
- **Customer Communication:** The backend must dispatch an automated email notifying the user of the cancellation, explicitly stating that ACH refunds take 1-3 business days to reflect in their linked bank account.

- **Inventory Sync:** The refund trigger must simultaneously release the held products back into the live inventory database to prevent lost sales on limited-release items.

3.6 User Portal & Account Management

3.6.1 Profile & Verification Status:

- A dedicated dashboard where users can view their current identity verification status (e.g., Unverified, Pending Review, Verified).
- If unverified or flagged, the portal provides a direct link to initiate or retry the third-party ID verification flow.

3.6.2 Active Orders & Handoff Tokens:

- A real-time view of all pending, queued, or in-transit orders.
- This section must prominently display the active QR Handoff Token required for physical delivery verification, as well as the live countdown timer for 24-hour in-store pickup reservations.

3.6.3 Order History (1-Year Retention):

- A historical log of completed transactions displaying the date, items purchased, and order total.
- For database optimization and to minimize the retention of sensitive data, this view is restricted to orders completed strictly within the trailing 12 months.

3.7 Admin Portal & Exception Management

3.7.1 Inventory Management:

- A secure interface allowing authorized Northern Legacy staff to add new products to the database, adjust pricing tiers, update live inventory counts, and manually toggle the "isLimitedRelease" promotional flags for special drops.

3.7.2 ID Verification Resolution Queue:

- A centralized dashboard that receives automated alerts when the third-party ID verification system flags a user's document for minor discrepancies (e.g., camera glare).

- Admins can manually review the flagged documents, cross-reference the data, and override the status to "Verified" or reject the application.

3.7.3 Delivery Exception Routing:

- A notification hub that intercepts issues originating from the driver application.
- If a driver tags an order as "Delivery Failed - ID Issue" at the dock or door, the admin portal instantly triggers a high-priority notification to management.
- This allows the staff to monitor the physical return of the product, track the 24-hour inventory hold, and assist the customer with their re-verification process.

4. User Flows

4.1 The "In-Store Pickup" Reservation (Happy Path)

1. **Selection:** User logs in, spots a product with a "Limited Time Availability" badge, and adds it to their cart to ensure they don't miss out.
2. **Fulfillment Choice:** During checkout, the user selects "In-Store Pickup" rather than a Land or Water delivery route.
3. **Payment Bypass:** Because pickup is selected, the system allows the user to bypass the mandatory ACH advance payment and select "Pay In-Store (Cash/Terminal)".
4. **Inventory Hold:** Upon order confirmation, the backend immediately deducts the product from the public live inventory. The order status updates to Awaiting Pickup, and a 24-hour countdown timer begins.
5. **Arrival & Verification:** The user arrives at Northern Legacy within the 24-hour window. A Northern Legacy associate requests their physical ID to ensure the person at the counter matches the verified profile that placed the reservation.
6. **Completion:** The user submits payment via cash or the physical card terminal. The associate marks the order as Completed in the Admin Dashboard, finalizing the transaction and permanently clearing the inventory hold.

4.2 The Maritime "Island Path" (Happy Path)

1. **Verification:** User registers from a seasonal cottage on Grindstone Island (US side). Scans driver's license or passport.
2. **Location:** User selects "Water Delivery."
3. **Address Input:** User cannot find an address; drops a pin on their dock. The system generates a Plus Code.
4. **Scheduling:** Calendar offers Thu, Fri, or Sat. User selects Friday.
5. **Payment:** User securely links their bank and completes an ACH advance payment (Cash option is disabled).
6. **Fulfillment:** System adds the fully paid order and Plus Code to the "Friday Water Route" manifest for the boat captain.
 - **Physical Verification (Driver Protocol):** The driver scans the physical ID and the QR code at the point of delivery to close the loop.

4.3 The "Canadian Overlap" (Unhappy Path)

1. **Selection:** A user at a dock in Gananoque, Ontario (4 miles away) attempts to order.
2. **Geocheck:** System calculates distance as 4 miles (Valid) but country as CA (Invalid).
3. **Error: Order is rejected.** Message: "*Sorry! We cannot deliver across international borders. Please visit us in Clayton for in-store pickup.*"

4.4 The "Missing ID" Protocol (Unhappy Path)

1. **Arrival:** The driver arrives at the scheduled Land or Water location and requests the customer's physical ID to complete the mandatory QR handoff scan.
2. **Verification Failure:** The customer cannot produce their physical ID, the ID is expired, or the QR handoff token fails to validate the recipient.
3. **Driver Action:** The driver aborts the handoff and tags the order as Delivery Failed - ID Issue in the driver application. The physical product is returned to the Clayton storefront.

4. **System Action (The 24-Hour Hold):** The backend updates the order status to Action Required and triggers an automated alert to the customer. The paid inventory is placed on a strict 24-hour hold.
 5. **Customer Remediation:** The customer must log into the Northern Legacy app, navigate to their blocked order, and complete a new ID upload flow to demonstrate they have physically located their valid ID.
 6. **Resolution: * Success:** Once the system verifies the newly uploaded ID, the order is automatically pushed back into the Pending Dispatch queue and assigned to the next available delivery window for their terrain type.
 - o **Failure (Refund Triggered):** If the customer does not complete the re-verification within the 24-hour hold window, the order is automatically Cancelled. The system triggers the Refund API to return the ACH payment (processing time 1-3 business days) and the product is returned to public inventory.
-

5. Non-Functional Requirements

5.1 Data Security & Retention

- **Encryption:** All data in transit must utilize TLS 1.3. Sensitive database fields must use AES-256 encryption at rest.
- **PII Minimization:** Raw image files of scanned IDs must be permanently purged from the server/cloud storage 30 days after verification to minimize liability.
- **Audit Retention:** While ID images are purged, anonymized transactional data and compliance logs must be securely retained for 7 years to satisfy OCM audit requirements.

5.2 Performance & Concurrency

- **Inventory Locking:** The database must utilize optimistic concurrency control (transaction locks) to prevent "overselling." If two users attempt to check out with the last unit of a limited-release item simultaneously, the system must strictly process the first request and gracefully decline the second.
- **Load Time:** The customer-facing menu must render its First Contentful Paint (FCP) in under 1.5 seconds on standard mobile LTE connections.

5.3 Resiliency & Offline Capabilities

- **Customer UI:** The interactive Map Picker must include a "Retry" function with intelligent timeout handling for users experiencing low cell signal on the river.
- **Driver UI (Offline Mode):** The driver-facing manifest and QR-scanning protocol must cache data locally (via Service Workers/Local Storage). This ensures the boat captain can successfully scan the customer's QR Handoff Token and physical ID at a remote dock even if they completely lose cellular connection, syncing the completion data to the database once a connection is re-established.

5.4 Compliance Auditing & Logging

- **Immutability:** Compliance logs must be append-only. To prevent tampering, these records cannot be edited or deleted by standard Admin roles.
- **Log Structure:** Every order must automatically generate a comprehensive log entry containing:
 - **Order_ID & User_ID**
 - **Device_Coordinates (Captured at the time of order placement)**
 - **Delivery_Plus_Code (For maritime routes)**
 - **ID_Verify_Ref_Number (Digital API Verification)**
 - **Driver_ID & Handoff_QR_Timestamp (Physical Verification)**

5.5 Accessibility (ADA Compliance)

- **Standard:** The customer-facing application must meet WCAG 2.1 Level AA compliance standards (e.g., proper contrast ratios, screen-reader compatible semantic HTML) to ensure accessibility for visually impaired users and mitigate ADA retail legal risks.