CASE STUDY – ONLINE GIVING PLATFORM

How a Leading Online Giving Platform Shut Down Card Testing at the Edge with Darwinium, and Kept Every Dollar Flowing to Charities

~70%
Of attempted payments interdicted

186,000+
Card-testing attempts rejected in a 90-day window

11,000
Card attempts from one device, caught

Summary of Results

- **Fast path to deployment.** Darwinium deployed on the platform's existing content delivery network (CDN) - AWS CloudFront, replacing the incumbent fraud tool with no changes to the donation forms.
- **Close to 70% of attempted payments interdicted.** More than 186,000 card-testing attempts rejected in a 90-day window, before they reached the payment processor.
- **Unprofiled API abuse eliminated.** Around 60% of payment attempts never touched a donation form. Every high-risk transaction is now blocked.
- **One device, 11,000 card attempts, caught.** A single device signature responsible for more than 20% of payment volume over 12 days was identified and shut down.
- **Strong fraud deterrent.** Rejected attempts receive a realistic decline, so tested cards look dead and attackers move on.

Digital Fundraising for High-Impact Nonprofits

The customer is a US-based online giving platform that provides nonprofits and charities the digital fundraising tools needed to grow. The platform is built to give donors flexibility in how, when, where and what they give, while making fundraising simpler for the organizations behind the cause.

That openness is also what makes donation platforms a target. Low-value, low-friction payments are exactly what fraudsters need to test stolen cards.

> "The speed and simplicity of deployment was a real benefit to us. The path to blocking card testing was extremely slick and we feel confident we are protecting the platform from even the most persistent abuse"
>
> Customer, Online Giving Platform

The Challenge: Card Testing at the Expense of Charities

Fraudsters use donation platforms, which typically have lower barriers to entry, to validate stolen credit cards with small payments, often as little as $5. If a transaction clears, the card is confirmed live and ready for resale or larger cash-outs elsewhere. Without effective detection, these payments sail through, and the cost lands on charities and the platform: processing fees on every attempt, potential chargeback fees, and the time and resources spent investigating.

The platform had an incumbent fraud tool in place for card testing, but needed to replace it quickly, and wanted a solution that could operate at the edge rather than in the application. Visibility was the deeper problem. Early analysis showed that around 60% of payment attempts carried no profiling at all. They came via a direct API route that never touched a browser or donation form, bypassing conventional controls entirely.

Browser traffic told a similar story: individual devices attempting dozens of cards in short succession, users clearing cookies to look new, mismatched browser signatures, captcha solvers and automated extensions.

THE PLATFORM SET THREE CLEAR GOALS:

01

Stop card testing at the payment step, before attempts reach the processor.

02

Deploy at the edge on the platform's existing AWS CloudFront infrastructure, fast.

03

Deceive, don't just decline. Return a realistic failure response so fraudsters believe the card is dead and stop coming back.

The Solution: Real-Time Payment Decisioning at the Edge

The platform partnered with Darwinium to protect its donation journeys at the edge. Darwinium was deployed on the platform's existing AWS CloudFront distributions, covering both the payment API and the embedded giving forms where donors are profiled. Because Darwinium runs natively at the CDN edge, every payment attempt is profiled, classified and decisioned in real time, whether it arrives from a browser or hits the API directly.

Darwinium returns a pass, challenge or reject decision for every payment, which the platform actions in its own backend for real-time decisioning. When Darwinium detects card testing, the platform presents the fraudster with a fake decline: a normal-looking API response carrying a genuine processor decline code. The card appears dead, the fraudster moves on, and the platform never pays a processing fee on the attempt.

Card Testing

Flagging devices attempting payments with multiple cards in a short period, and returning a realistic decline.

Direct API Abuse

Blocking 100% of unprofiled payment attempts that bypass the donation form unless they are allow-listed.

Device Churning

Linking users who clear cookies or local storage back to the same device through signature matching.

Agentic and Automated Traffic

Detecting Captcha solvers, agentic AI extensions and AI-agent cadence, while letting legitimate agent-assisted donations through.

Key Darwinium Capabilities Used

Edge Deployment on AWS CloudFront

Profiling and decisioning run at the CDN edge across the payment API and giving forms, with no application changes.

Device Intelligence

Fuzzy device signatures recognize the same device across cleared cookies, rotated storage and multiple cards.

Browser Integrity Signals

Mismatches between the browser reported by JavaScript and by device data expose spoofed or automated clients.

Agentic AI Detection

A behavioral model flags the unnaturally uniform event cadence of AI agents, alongside captcha solvers and automation extensions.

Flexible Decision Strategies

Layered rules drive pass, challenge or reject outcomes that the platform consumes in real time and can tune without heavy engineering.

Honey-Trap Responses

Rejected attempts return a realistic decline, turning detection into deterrence.

Impact Highlights

Direct API Abuse Shut Down

- Around 60% of payment attempts arrived with no profiling and never touched a donation form. The platform now blocks 100% of this direct traffic unless it is allow-listed.

Card Testers Exposed by Device

- Devices flagged for card testing averaged around 60 card attempts per device signature.
- One device signature attempted more than 11,000 card payments over 12 days, more than 20% of the platform's total payment volume in that period. Its behavioral signature, activity duration and storage identifiers were nearly fixed throughout, indicating a replayed, stale profiling session. It was identified and blocked.

Processing Fees Avoided

- Darwinium's decisioning engine interdicted close to 70% of attempted payments: 186,063 rejected card payments between 28 June and 28 September.
- Every rejected attempt is a processing fee that was never paid, meaning hundreds of thousands of dollars saved in operational costs.

Device Churning Defeated

- Nearly 15% of device signatures, around 8,500 devices, belonged to users who had cleared cookies or local storage. Darwinium's signature matching linked them back to the original device.
- Darwinium detected a browser mismatch between JavaScript and device data in 20% of browser payments, around 25,000 attempts. 65% of these were flagged by the platform's rules.

Automation and AI Agents Identified, Not Blanket-Blocked

- Nearly 500 payments came from end users running a captcha solver or agentic AI browser extension.
- 5.5% of browser-based payment attempts were flagged as likely AI agents, based on an unnaturally uniform cadence of events, compared with 1–3% at other Darwinium customers.
- Only 21% of agent-flagged payments were blocked, against a 70% block rate across all payments, so legitimate agent-assisted donations can still get through.

Looking Ahead

With Darwinium now the real-time decision engine for every payment, the platform is moving from blocking card testing to refining it. Next steps include feeding the platform's own truth data back into Darwinium to sharpen rule accuracy and reduce false positives, and quantifying the full cost of fraud avoided across processing fees, chargebacks and investigation time.

Together, the customer and Darwinium are showing that a giving platform can stay open and frictionless for donors, and for the AI agents increasingly helping them, while closing the door on the fraudsters who exploit generosity.

About Darwinium

Darwinium is the Intent Intelligence Company, built to protect and grow revenue at every touchpoint by understanding user behaviour and intent. Its edge-based risk decisioning platform distinguishes trusted from risky human and AI behaviour across the entire customer journey, resulting in 50% less fraud and 40% greater operational efficiency. From first interaction through high-risk actions and payments, Darwinium protects the moments that matter most, so digital leaders can confidently grow and protect revenue. Learn more at **darwinium.com**