MCP SERVER | NO CODE | CLOUD HOSTED

Mastercard MCP

Get instant payment intelligence from any location.

Mastercard MCP gives your AI client instant access to global payment intelligence. Identify card issuer details from the first few digits (BIN lookup), validate account status before transactions, locate specific merchants using GPS coordinates or street addresses, and report confirmed fraud cases directly. It's a single connection point for everything related to modern commerce payments.

A+ Quality Score 98.33/100

bin-lookup | fraud-detection | card-validation | merchant-services | financial-data

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/mastercard

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Mastercard MCP

12 tools available
Cloud-hosted on Vinkius

Mastercard connects deep payment infrastructure capabilities directly to your agent through this MCP. You get instant intelligence on cards, merchants, and transactions without having to jump between complex developer portals or write boilerplate API code. Need to know if a card is active before processing a charge? Ask the AI. Trying to find a restaurant that takes contactless payments nearby? The MCP handles the geospatial search and payment capability filtering automatically.

This isn't just another data dump; it’s a conversational layer over global financial rules. You can determine everything from business classification using MCC codes to finding detailed merchant information, all through simple conversation with your AI client. Connecting this via Vinkius means you get immediate access to the full suite of payment tools, letting your agent act like an expert payments analyst on demand.

Core Capabilities

01 — Determine card issuer and type

Read the first 6-8 digits of any card number to instantly identify the bank that issued it, whether it's credit or debit, and its specific premium category.

02 — Validate account status

Check if a full payment card number is currently active and valid before initiating any transaction, preventing costly declines.

03 — Find merchants by location or address

Search for Mastercard-accepting businesses near specific GPS coordinates or using a user-friendly street address input.

04 — Identify local payment capabilities

Discover nearby locations and pinpoint if they accept digital wallets like Apple Pay, Google Pay, or contactless methods.

05 — Report confirmed fraud cases

Submit details of a fraudulent transaction to Mastercard's database for network protection and analysis.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/mastercard** — connect your AI agent in three steps.

01 Subscribe to the MCP and provide your Mastercard Developer Client ID and Client Secret.

02 Your AI client uses natural language to formulate a request, specifying what it needs—for example, 'Find restaurants near 34th Street that accept digital wallets.'

03 The MCP executes the necessary background calls, gathers data on merchants or card details, and presents the final answer directly back through your agent.

The bottom line is you never have to write a single API call yourself; you just ask your AI client what payment intelligence you need.

Built For

This MCP is critical for anyone whose daily job involves verifying financial data or locating physical points of sale. It's built for fraud analysts who need to investigate suspicious activity fast, and e-commerce operators struggling with high payment decline rates.

Fintech Developer

Building checkout flows that must validate card numbers or determine optimal payment routing before processing a charge.

Fraud Analyst

Investigating flagged transactions by running BIN lookups to check issuer details and submitting fraud reports for suspicious activity.

Travel & Concierge Service Agent

Helping clients find specific types of local businesses, ensuring those merchants accept modern payment methods like digital wallets or contactless pay.

What Changes When You Connect

01 Reduces transaction decline rates by running accounts through the `validate_account` tool, ensuring you only process payments on active cards. This saves time and money immediately.

02 Finds merchants using either coordinates (`search_merchants`) or a simple street address (`search_places_by_address`), making location queries much more user-friendly for any client.

03 Quickly identifies card details using `bin_lookup` , letting your agent tell you the issuer bank, card tier (Gold/Platinum), and country from just the first few digits of a number.

04 Enhances customer service by searching for locations that accept specific digital wallets. Use `search_places` to filter results specifically for Apple Pay or Google Pay support.

05 Improves compliance workflows by allowing authorized personnel to use `submit_fraud_report` , feeding confirmed fraud data back into the network immediately.

Real-World Applications

A traveler needs a local store that accepts digital payments.

The user asks: 'Where's a coffee shop near me that takes Apple Pay?' The agent uses `search_places` with the current GPS coordinates and filters for Apple Pay acceptance, returning precise results.

A fraud analyst needs to investigate suspicious transaction batch data.

The user asks: 'What is the issuer bank behind these card numbers?' The agent runs `bin_lookup` on the partial number, immediately telling the analyst if it's a corporate or prepaid account.

An e-commerce developer needs to validate customer inputs before checkout.

The user asks: 'Is this card number active?' The agent executes `validate_account` with the full PAN, giving a definitive VALID/INVALID status so the payment gateway doesn't waste time.

A sales team needs to find potential retail partners in a new district.

The user asks: 'Show me all local restaurants near 123 Main St.' The agent uses `search_places_by_address` and then uses the resulting IDs with `get_place_details` to pull complete contact info.

Patterns to Avoid

Searching for merchants without a location.

✗ AVOID

Asking, 'Where can I find a gas station?' The system cannot answer because the tool requires coordinates or an address to define the search area.

✓ INSTEAD

Always provide context. Instead of asking generally, ask: 'Find gas stations near 34th Street.' Use `nearby_locations` or `search_merchants` with specific GPS data.

Assuming card type from the number.

✗ AVOID

Looking at a partial number and guessing if it's debit, credit, or prepaid. This is unreliable and risks transaction failure.

✓ INSTEAD

Use `bin_lookup` to get a definitive breakdown. It tells you the exact card category (Standard/Gold) and whether it’s commercial or consumer.

Trying to analyze raw MCC codes manually.

✗ AVOID

Getting a list of 4-digit MCC codes and trying to figure out what they mean. The codebook is massive and hard to read.

✓ INSTEAD

First, use `merchant_category_codes` or `merchant_industry_codes` to understand the classification hierarchy before filtering your searches.

The Right Fit

Use this MCP if your primary need is *intelligence* about transactions, locations, or businesses. If you are validating a card number, you must use `validate_account`. If you are finding physical places, always start with location-based tools like `search_merchants` or `search_places_by_address`, as these provide the necessary coordinates to make sense of the data. Don't use this if your goal is simply retrieving a static list of all global MCC codes; for that, just call `merchant_category_codes`. You shouldn't rely on this MCP if you only need basic contact information without payment acceptance details—you might be better off using a simple directory API instead. This tool is specialized for the complex intersection of commerce and finance.

The pain of fragmented payment data

Today, if you need to know what kind of card a customer has or where they can spend it, you hit multiple roadblocks. You might check one API for BIN lookup, then switch to a separate map service to find the physical store, and finally use a third portal just to see if that location accepts Apple Pay. It’s copy-pasting coordinates into five different tabs until your agent throws an error.

With this MCP, all of that complexity disappears. You tell your AI client the goal—for instance, 'Find me a merchant near downtown that takes digital wallets.' Your agent runs through the necessary checks using `search_places`, confirms payment methods, and gives you one clean answer. It just works.

Mastercard MCP: Location Search and Validation

Before this MCP, finding a business meant guessing its location type or relying on manual cross-referencing of MCC codes against local directories. You couldn't easily tell if a merchant accepting credit cards was also set up to handle Apple Pay.

Now, your agent handles the entire query sequence automatically. It combines geographic searching with payment capability checks in one conversational step. The intelligence is immediate and actionable.

Mastercard MCP: 12 Tools for Payments

These twelve tools give your AI agent the ability to perform complex tasks like card validation, merchant discovery, and fraud reporting through simple conversation.

#	TOOL	DESCRIPTION
01	bin_lookup	Identifies a card's issuer bank, type (credit/debit), and category using only the first 6 to 8 digits of the card number.
02	bin_lookup_post	Performs the same card identification lookup as bin_lookup but uses a POST method, which is better for handling sensitive payment data.
03	get_merchant	Retrieves detailed information, including hours and accepted methods, for a specific merchant identified by its unique ID number.
04	get_place_details	Gets complete details, like coordinates and payment types, for any location found during a nearby places search.
05	merchant_category_codes	Provides a comprehensive list of all four-digit Merchant Category Codes used to classify every type of business.
06	merchant_industry_codes	Lists higher-level industry codes, grouping related MCCs for broader market analysis and business classification.
07	nearby_locations	Discovers general points of interest, including ATMs or merchants, within a given radius from specific GPS coordinates.
08	search_merchants	Finds Mastercard-accepting businesses near GPS coordinates and allows filtering by business type (MCC code).
09	search_places	Searches for nearby locations using GPS, specifically filtering results to show which ones accept Apple Pay or Google Pay.
10	search_places_by_address	Finds specific merchant places by providing a street address instead of raw coordinates.
11	submit_fraud_report	Allows authorized users to submit confirmed fraudulent transaction details directly to Mastercard’s loss database.
12	validate_account	Checks a full card number against the network to confirm if it is currently active and valid for immediate transactions.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U What type of card is 542418 and which bank issued it?

Running BIN lookup for 542418... This is a Mastercard World Elite credit card issued by Banco Exemplo S.A. in Brazil. It's a premium tier card (not prepaid, not commercial) with BRL as the primary currency. The BIN range covers 54241800 to 54241899.

U Find restaurants near São Paulo city center that accept Mastercard within 3km.

Found 27 restaurants within 3km of São Paulo center. Top results include: Restaurante Paulista (MCC: 5812) at Av. Paulista, 500; Sabor Brasileiro on Rua Augusta, 1200; and Pizzaria Bella on Rua Oscar Freire, 800. All accept Mastercard. Would you like details on any specific restaurant?

U Validate card number 5123456789012346 before I process this payment.

Card validation complete: **2346 is VALID. Account type: Credit card. Issuer: First National Bank. The card is active and ready for transactions. You can proceed with processing this payment safely.

Frequently Asked Questions

01 **Can I identify what bank issued a card just from the first few digits?**

Yes! Use the `bin_lookup` tool with the first 6-8 digits of the card number (the BIN). Mastercard will return the issuer bank name, card type (credit/debit/prepaid), card category (Gold/Platinum/World), issuing country, and flags like whether it's a commercial or healthcare card. For example, BIN 542418 reveals the exact issuing bank and card tier.

02 **How can I find merchants that accept Mastercard near a specific location?**

Use the `search_merchants` tool with latitude, longitude, and a search radius in meters. You can optionally filter by MCC code (e.g., "5812" for restaurants, "5411" for grocery stores). For example, searching with coordinates -23.5505, -46.6333 (São Paulo) and radius 5000 will return all Mastercard-accepting merchants within 5km. Results include merchant names, addresses, categories, and coordinates.

03 **Can I verify if a payment card is valid before processing a transaction?**

Yes! Use the `validate_account` tool with the full card number. It checks Mastercard records to determine if the card is active and valid, returning the validation status (VALID/INVALID), account type (credit/debit/prepaid), and issuer information. Optionally include expiry date (MMYY format) and cardholder name for enhanced validation. This helps reduce declined transactions and fraud risk. Never store full card numbers — handle them securely.

04 **How do I report a confirmed fraudulent transaction to Mastercard?**

Use the `submit_fraud_report` tool with the card number, transaction amount, currency (ISO 4217), and fraud type code. Fraud types: "01" = Stolen Card, "02" = Never Received Card, "03" = Fraudulent Application, "04" = Counterfeit Card. Optionally include fraud amount and transaction date. This submits to Mastercard's Fraud and Loss Database (FLD) to help reduce false positives across the network. IMPORTANT: Only authorized fraud management personnel should use this tool for confirmed cases.

05 **Can I find merchants that accept Apple Pay or Google Pay near me?**

Yes! Use the `search_places` tool with GPS coordinates and set hasApplePay=true or hasGooglePay=true to filter for merchants with those payment capabilities. Returns detailed merchant information including names, addresses, MCC codes, and which digital wallets they accept. For example, searching near Times Square (40.7580, -73.9855) with hasApplePay=true will show all nearby Apple Pay-enabled merchants.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"mastercard": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Mastercard is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Mastercard. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Mastercard MCP
Server ID	`019d75d0-036e-71cd-91de-74e97c087863`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/mastercard.