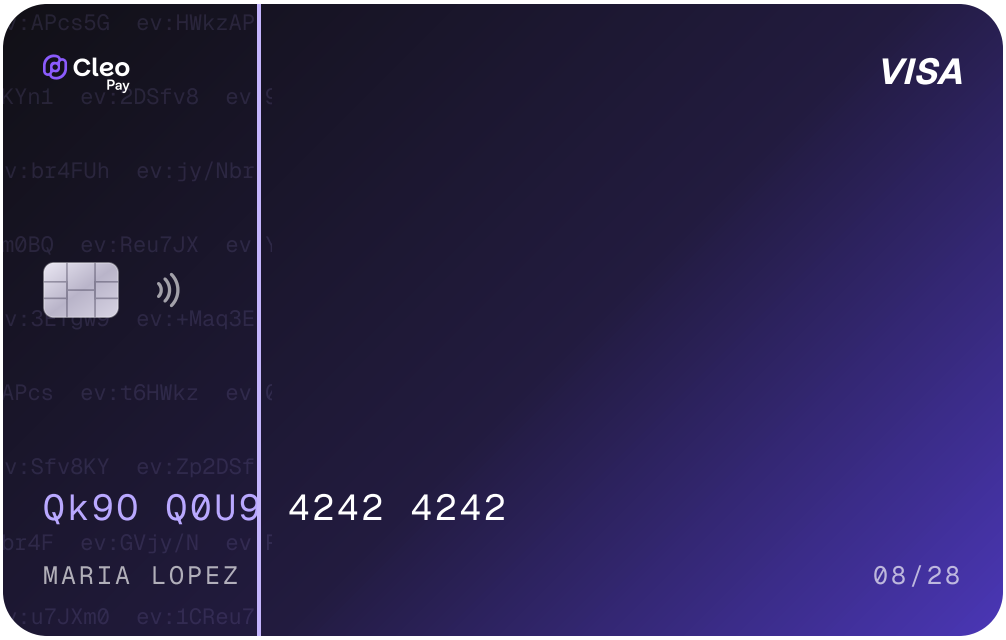
Cleo Pay

Your clients' cards, encrypted before they reach us.

Clients enter cards on a secure form from Evervault, our PCI DSS Level 1 service provider. The number is encrypted in their browser, so Cleo's servers never see it.



HOW IT WORKS

How a card moves through Vault.

From the request link to a reveal, the plain card number never touches Cleo's servers.

1 **Request** | 2 Encrypt | 3 Store | 4 Reveal

You send your client a request link. They enter the card on a secure form hosted by Evervault.



ENCRYPTION

What “encrypted” usually means.

Most apps say client cards are encrypted. That usually means two layers that still let the app read the card. Vault adds a third.

IN TRANSIT

Encrypted on the way.

HTTPS protects the card between the browser and the app. When it arrives, the app's server decrypts it and handles the plain number.

The app sees the card

AT REST

Encrypted on disk.

The database and its backups are encrypted. The app holds the key, so it can read the card back whenever it runs.

The app sees the card

AT CAPTURE

Encrypted before it leaves the browser.

Evervault encrypts each field on your client's device with AES-256-GCM. The keys stay in Evervault's hardware-isolated enclaves, and Cleo's servers hold no key to decrypt the card.

Cleo never sees the card

COMPARISON

The usual way, compared with Vault.

Most agencies keep client cards in email, PDFs, and spreadsheets. Apps that store cards often receive the plain number and hold the keys too. Either way, one leaked password or server exposes full cards.

	THE USUAL WAY	VAULT
Where the card is encrypted	On the app's servers after the plain card arrives, or not at all	In the client's browser, before it reaches Cleo
Who holds the keys	The app or agency, which must store and rotate them	Evervault, our PCI DSS Level 1 service provider
What the database holds	Full card numbers, or encrypted numbers next to their keys	Encrypted values, plus brand and last 4
Where cards are decrypted	On the app's servers	At Evervault, then shown in the agent's browser
Security codes	Often kept indefinitely	Cleared after 30 days, or up to 90 if you choose
Who can see a full card	Anyone with the inbox, file, or account	Agents with reveal permission, and every reveal is logged

ACCESS

Only the right people see a full card.

You decide who sees which clients and who can reveal a card. Vault keeps a record of every reveal.

Agents see only their clients.

Admins see every client. Agents see the clients assigned to them.

Revealing a card is its own permission.

Cards stay masked in the app. Only people you give reveal permission can see a full card number.

Every reveal is logged.

Vault records who revealed which card, when, and from what IP address and device, before the card is shown. Admins can review the log anytime.

RETENTION

Card data has an end date.

PCI DSS does not allow keeping a security code after it is used, so Vault clears it for you.

Security codes clear on their own.

Vault clears each security code 30 days after it is added, or after up to 90 days if you choose. Each clearing is logged.

Request links expire and work once.

Pick an expiry from 4 hours to 7 days. A link stops working once your client submits a card, and every submission passes a bot check.

Deleting removes the card.

Deleting a card or a client removes the encrypted card number and security code, and cancels that client's open request links.

QUESTIONS

Security questions.

Does Cleo store credit card numbers?

Yes, but only as ciphertext that our servers can't decrypt.

When your client adds a card. They type it into Evervault's secure form, and it is encrypted in their browser. Cleo receives only the encrypted value.

In our database. We keep that ciphertext plus the brand, last 4, expiry, cardholder name, and billing address. Cleo's servers hold no Evervault decryption key.

When an agent reveals a card. Cleo checks the agent's permission and logs the reveal. Evervault then decrypts the card on its way to that agent's browser.

Is Vault PCI compliant?

Vault's card data is held to PCI DSS Level 1. Every card is encrypted and stored by Evervault, our PCI DSS Level 1 service provider.

Independently assessed. A Qualified Security Assessor reviews Evervault every year with a full Report on Compliance under PCI DSS v4.0.1. It covers the card form and Relay, the Evervault services Vault uses.

Kept off Cleo's servers. Cards are encrypted in your client's browser, so plain card numbers never reach our systems.

For your agency. Your agency keeps its own PCI DSS obligations. Keeping cards in Vault instead of email or spreadsheets keeps full numbers out of your inboxes and files, and you can download Evervault's Attestation of Compliance at cleo-pay.com/vault/security for your records.

How is card data encrypted?

In your client's browser, before it reaches us. Evervault encrypts the card number and security code with AES-256-GCM on their device. The keys stay in Evervault's hardware-isolated enclaves, and every connection to Cleo uses HTTPS.

Can Cleo employees see our clients' cards?

No. Our servers only hold encrypted card data and have no key to decrypt it.

Does Vault keep card security codes?

Only for a limited time. Vault clears each security code 30 days after it is added, or after up to 90 days if your agency sets it.

Can we see who looked at a card?

Yes. Every reveal is logged with the person, the card, the time, the IP address, and the device. Admins can review the log anytime.

What happens when an agent leaves?

Remove them from your team and they lose access right away. Their reveal history stays in the log.

Where is Vault hosted?

In the United States. Cleo's app and database run in a US East data center, and Evervault holds the encryption keys in hardware-isolated enclaves on AWS.

Can we get compliance documents for our review?

Yes. Download Evervault's PCI DSS Attestation of Compliance and our security overview at cleo-pay.com/vault/security. For your security questionnaire, email support@cleo-pay.com.

How do I report a security issue?

Email support@cleo-pay.com with what you found and how to reproduce it.
