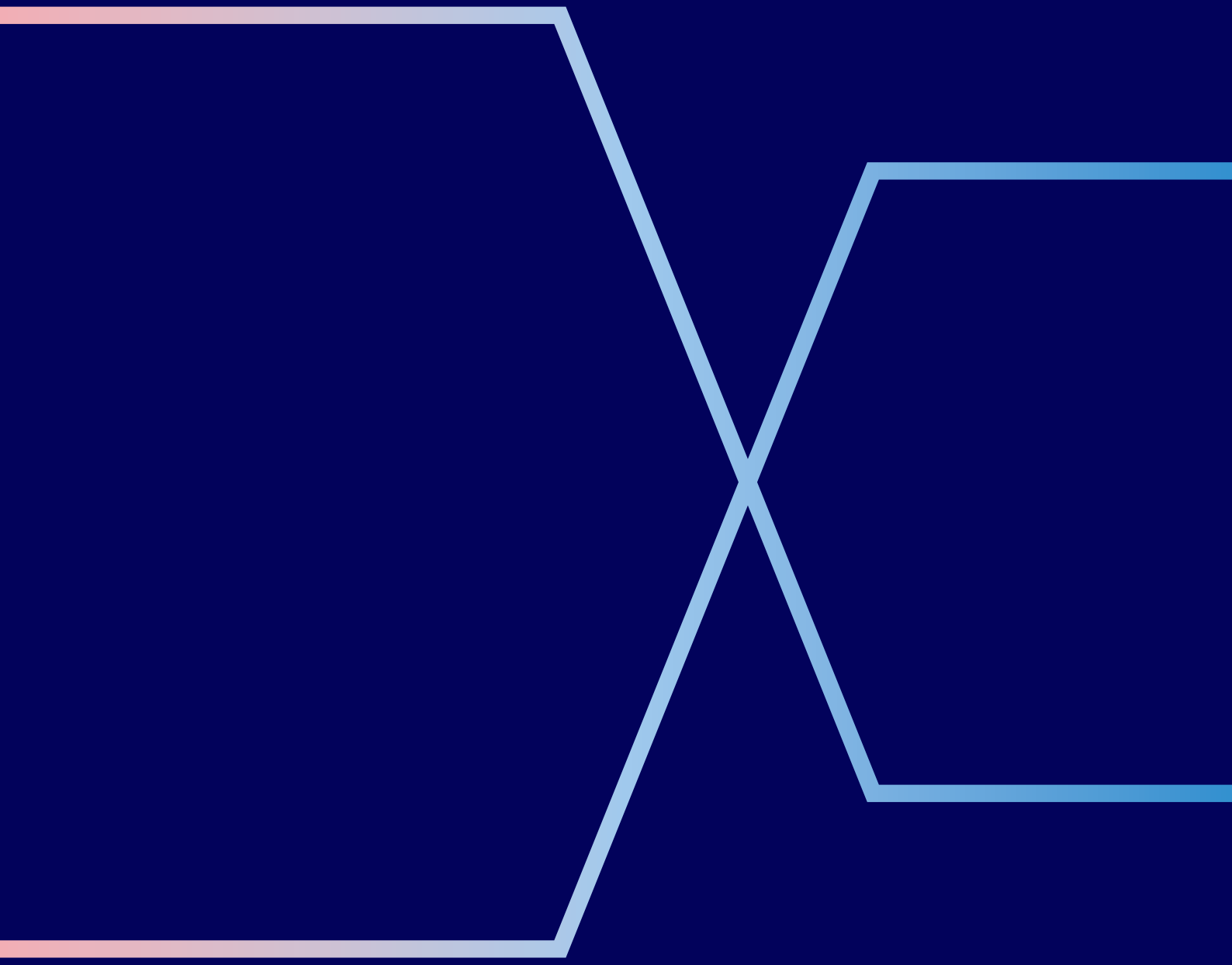
Retailers

Best practice for avoiding and managing chargebacks.



elavon®

This guide outlines practical advice for retailers to reduce chargebacks, protect revenue, and respond effectively to disputes. You should use it to train staff, review internal processes and prepare documentation.

General guidance

Always use the safest payment method: Chip & PIN or contactless, or use 3D Secure online. Avoid manual entry wherever possible. Train staff to spot mismatches between how a card was entered and what the receipt says.

Set up email chargeback alerts so you never miss a notification.

- Using a shared inbox, e.g. disputes@yourcompany com could help to avoid delays during staff absences.
- Whitelist the email address **elavondisputes@elavon.com** to make sure our messages reach you and check spam folders regularly.

Reply on time to all chargebacks. Never miss the “Respond By” date – especially around holidays or busy periods.

Avoid additional refunds once a chargeback is issued. Accept the case or provide a full defence, but make sure you don’t double-pay.

Keep your merchant details updated, including trading names and addresses, to avoid disputes due to confusion or mismatched info.

Provide clear, disclosed Terms & Conditions and refund policies.

- Face-to-face: include on receipt or get signed consent.
- Mail order/telephone order (MOTO): send terms by email and get written confirmation.
- E-commerce: use clear click-to-accept boxes with visible terms and refund info.

Avoid links or cloud-based files when submitting evidence. Use PDFs, images or text files only.

Prepare standard response packages with Ts & Cs, refund policies, screenshots, and user guides to make defending cases easier.

Make sure customer records link clearly to payments and transactions — including third-party bookings.

If the customer and cardholder are different, keep both sets of details.

Fraud prevention

Train staff on chargebacks, so frontline teams understand how disputes work and feel confident in knowing how to spot risks and unusual behaviour.

Use secure transaction methods.

- CHIP & PIN or contactless for in-person.
- 3D Secure for online.
- Avoid manual card entry unless absolutely necessary.

Disable manual entry if not needed for MOTO transactions and switch instead to secure pay-by-link methods where possible. Use fraud filters and Address Verification Service (AVS)/Network Access Control (NAC) checks. If the check fails, consider declining the payment. Process refunds correctly always refund the original card used. Don’t use cash, bank transfer, or a different card.

Set up fraud screening and take immediate action on high-risk transactions.

Save evidence linking the booking, customer, and payment.

Authorisation issues

Don't force transactions if the card is declined. Make sure you follow prompts carefully: if a voice referral is requested, call the number provided. Don't treat it as a PIN request.

Use authorisation codes only when issued by the system, never accept authorisation codes from customers. Use authorisation codes only once and don't reuse or reverse codes after a transaction has been completed. If the amount changes, process a new sale and document the difference.

Avoid splitting transactions to bypass limits — this can trigger disputes.

Avoid using debit cards for pre-authorisation, except for verifying the card with a very low value transaction (£0.01)

Processing errors

Always use the correct refund method, onto the same payment card.

- Void" or "Reversal" for open batch transactions.
- Full refund for closed batch issues.
- Use the same currency chosen by the customer and display the conversion rate clearly at the point of sale.

Monitor for duplicate transactions using Elavon Connect and issue prompt refunds if found.

Respond with full documentation for duplicate charges or "paid by other means" claims — invoices, receipts, and system logs.

Customer disputes

Keep a record of complaints and your response, even if the issue was resolved.

Have a standard dispute pack ready with order confirmation, screenshots and website screen showing click-to-accept.

Card transaction cycle

Customer chooses to **make a purchase**

Customer **inserts/taps** card or enters card details **online**

Merchant sends payment data **requesting authorisation**

Acquirer/gateway routes the data to the **appropriate card network**

Card network (Visa/ Mastercard/Amex) **checks and forwards** to relevant card issuer

Card issuer **approves/ declines** the payment and sends a response

Acquirer **deposits funds** into merchant account

Merchant **gets paid**, minus any fees

Customer **receives purchase**

Chargeback transaction cycle

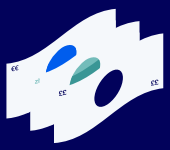
Customer **disputes a payment** with their bank

Issuing bank **pulls money back**

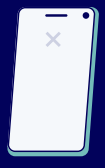
Card network **applies rules & deadlines**

Issuing bank **reviews decision**

If customer is **successful**, the refund stands



If merchant **defends** successfully, money is returned



Acquiring bank **passes claim** to merchant

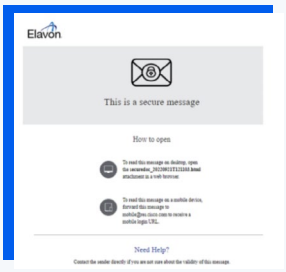
Merchant either: accepts **loss or** sends **evidence**

Contact us for more information
UK 0345 850 0195 chargebacks@elavon.com elavon.co.uk
IRE 1850 202 120 chargebacks@elavon.com elavon.ie

How to create a secure email account

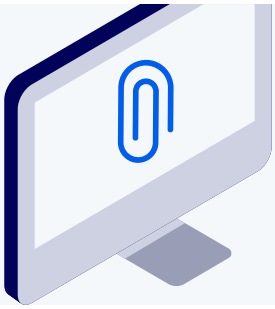
If a chargeback is raised against your business, we'll notify you by secure email. To view these messages, you will need to register your email address - here's how. You only need to do this once.

1



Look out for an email from **disputes@Elavon.com,** and save it to your device

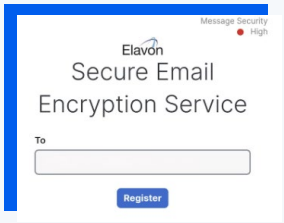
2



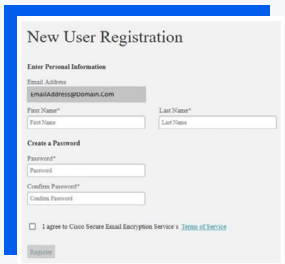
Click to **open the attachment** in your web browser.

3

Register your e-mail address with Cisco.

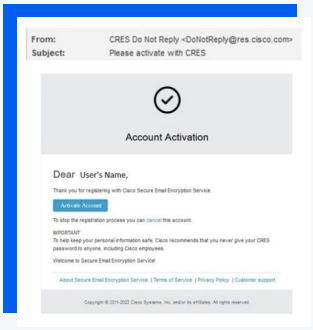


Complete each field in the form and click continue to submit. You should see a confirmation page



4

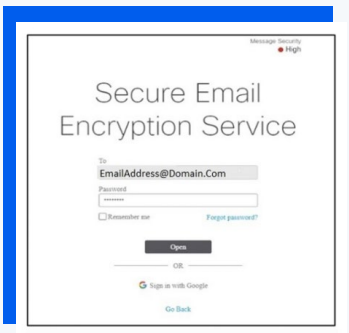
Check your email account for an email, with a button to **activate your account.**



The email will be sent from **"DoNotReply@res.cisco.com"** and will have a **"Please activate with CRES"** title. Activate Your Cisco Registered Envelope Service Account. You may need to check your Junk folder.

5

Return to the **registered envelope**. The Register button has been replaced with an **Open button** and you will be prompted for a password.



Enter the password for your Cisco Registered Envelope Service user account and **click the Open button.**