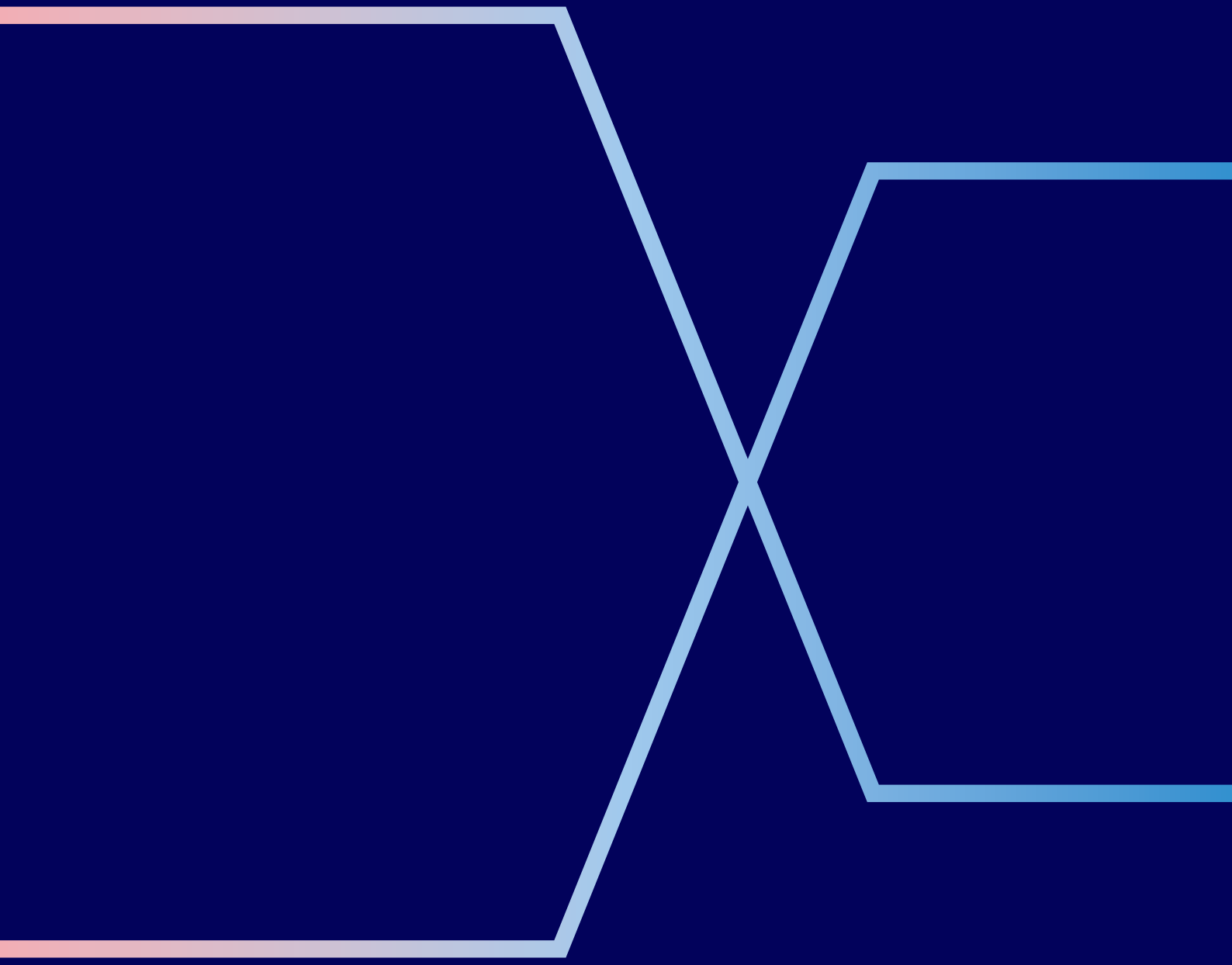
Service-led businesses

Best practice for avoiding and managing chargebacks.



elavon®

This guide outlines practical advice for all kinds of service-led businesses 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

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.

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

Process refunds correctly always refund the original card used. Don't use cash, bank transfer, or a different card.

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 Ts & Cs and refund policies.

- Face-to-face: include on receipt.
- MOTO: send terms by email and get written confirmation.
- E-commerce: use clear click-to-accept boxes with visible terms and refund info.

Link each transaction to customer details so you can trace it quickly if challenged.

If the cardholder and service user differ, keep both sets of details.

Fraud prevention

Use secure transaction methods.

- CHIP & PIN or contactless for in-person.
- 3D Secure for online.
- Avoid manual card entry unless absolutely necessary.
- Use Pay-by-Link instead of taking card details over the phone.

Train staff to spot unusual behaviour, especially attempts to distract during payment or enter details manually.

Disable manual entry if not needed for Mail order/telephone order (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.

Don't relax security for B2B or group bookings — apply the same fraud checks.

Pre-authorising £0.01 with 3D Secure at booking can reduce risk, especially for no-shows. Take action on high-risk transactions — continuing is at your own risk.

Third-party booking platforms do not guarantee security — always verify bookings yourself.

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 increases, complete the original authorisation and charge the remainder separately — and document it clearly.

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

Avoid using debit cards for pre-authorisation (except a small amount to confirm the card is real).

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 any are found.

Use separate invoices for repeat visits or additional charges to avoid duplicate payment disputes.

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

Customer disputes

Keep a standard document pack ready for disputes, containing booking terms, refund policy, signed agreements, and website screenshots.

Keep a record of all complaints, resolutions and customer correspondence — especially for claims like "service not as described". Provide full evidence of any resolution steps taken.

Additional charges (e.g. damage, extra services) must always be authorised — ideally by PIN or written consent.

If using third-party sites, make sure their Ts & Cs and booking pages meet card scheme rules (especially Visa).

If using virtual cards (issued by agencies), understand their terms override yours. Charge extras to the customer's own card, not the virtual one. To check if a chargeback came from the guest or agency, review any documents or logos included in the notification.

If the issue involved misconduct, record everything. If police were involved, include a reference number or confirmation.

If service was interrupted by external issues (like weather or disruption), show proof of how it was resolved, and reference your Ts & Cs at time of booking.

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

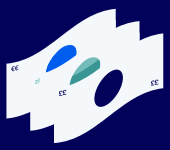
Customer **disputes a payment** with their bank

Issuing bank **pulls money back**

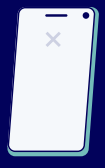
Card network **applies rules & deadlines**

Issuing bank **reviews decision**

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



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



Acquiring bank **passes claim** to merchant

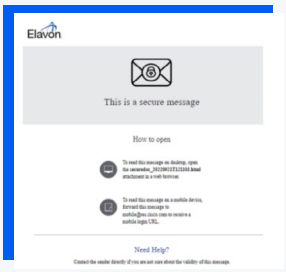
Merchant either: accepts **loss or** sends **evidence**

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

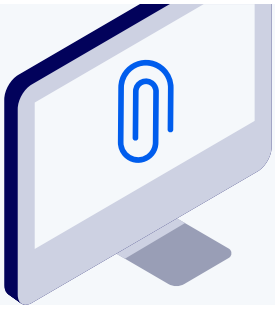
If a chargeback is raised against your business, we'll notify you by secure email. To view these messages, you will need to register your email address - here's how. You only need to do this once.

1



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

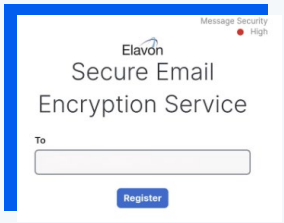
2



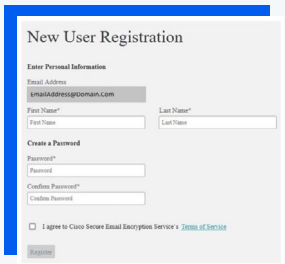
Click to **open the attachment** in your web browser.

3

Register your e-mail address with Cisco.

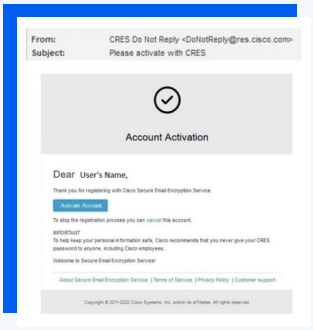


Complete each field in the form and click continue to submit. You should see a confirmation page



4

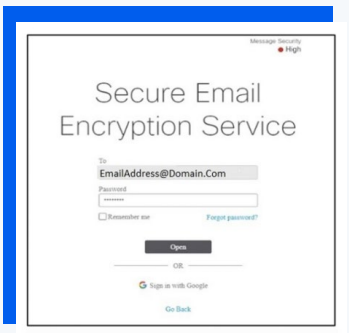
Check your email account for an email, with a button to **activate your account.**



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.**