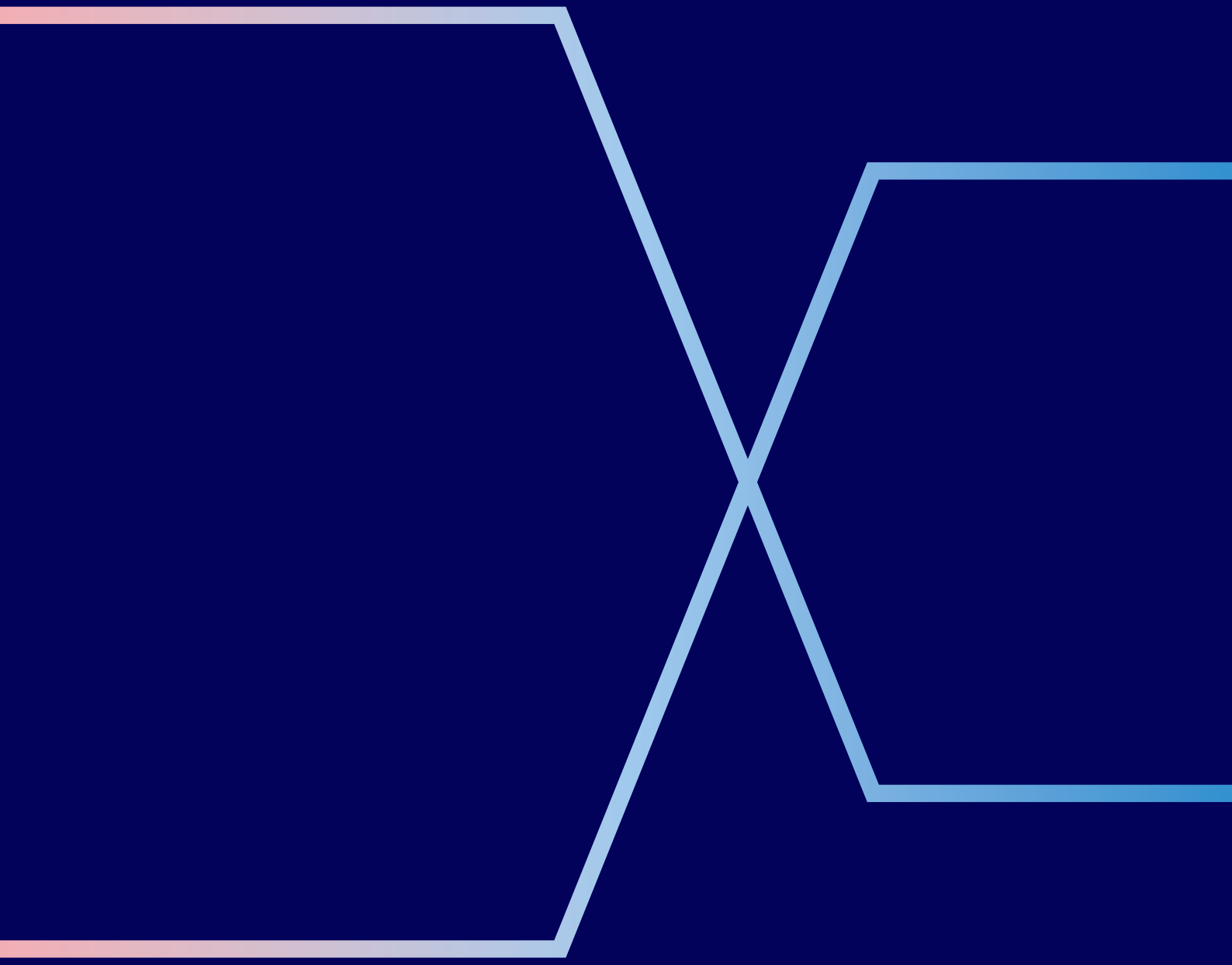
Restaurants, bars and food sellers

Best practice for avoiding and managing chargebacks.



elavon®

This guide outlines practical advice 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 Terms & Conditions 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.

Fraud prevention

Use secure transaction methods.

- CHIP & PIN or contactless for in-person.
- 3D Secure for online.
- Avoid manual card entry unless absolutely necessary.
- For phone orders, use Pay-by-Link to secure the transaction.

Set up fraud filters and don't ignore warnings — you take the risk if you go ahead with flagged payments.

For no-show bookings, pre-authorise a small amount (e.g. £0.01) with 3D Secure at the time of reservation. If a card was taken insecurely, follow up with a secure pre-authorisation or PIN-based purchase on arrival. Avoid pre-authorising debit cards unless it's just a £0.01 verification.

Train staff to check receipts: if the card was swiped but the receipt says "PIN Verified" or "Keyed", cancel and retake the payment securely.

Link bookings, payments, and customer data so it's easy to track transactions if a dispute happens.

Don't reduce fraud checks, even for business or group bookings. These types of transactions can still be fraudulent.

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

Bookings made through third-party platforms aren't guaranteed secure — always run your own checks.

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.

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

If the final bill is higher, complete the original and charge the extra as a new, documented transaction.

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.

If a customer queries a possible duplicate, confirm with Elavon or identify the transaction on your reports before replying.

If the bill is split or extended, issue separate invoices to avoid duplicate claims.

Customer disputes

Document all complaints and how you responded — especially if the customer was satisfied.

Extra charges (e.g. damages or add-ons) must be authorised by the customer — ideally via PIN or written consent.

Prepare a standard dispute pack including screenshots showing the booking process, Ts&Cs and refund policy, and show your click-to-accept box or signed agreement.

If you use third-party booking sites, check their page has a click-to-accept box — otherwise, your Ts&Cs might not apply.

For agency bookings with virtual cards, remember: their terms override yours. Add-on charges must go on the customer's card, not the agency's.

If you're unsure whether the chargeback came from the guest or an agency, check for branding in the documents.

If a customer caused disruption (e.g. abusive behaviour), document everything — and include police details if available.

For cancellations due to external issues (e.g. natural disaster), show how you resolved it and reference your Ts&Cs.

Keep a record and evidence of all complaints, resolutions and customer correspondence — especially for claims like "service not as described".

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

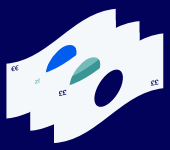
Customer **disputes a payment** with their bank

Issuing bank **pulls money back**

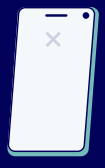
Card network **applies rules & deadlines**

Issuing bank **reviews decision**

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



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

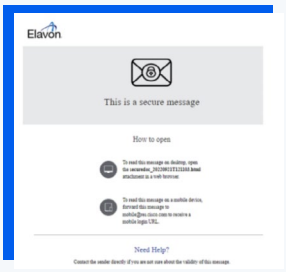


Contact us for more information
UK 0345 850 0195 chargebacks@elavon.com elavon.co.uk
IRE 1850 202 120 chargebacks@elavon.com elavon.ie

How to create a secure email account

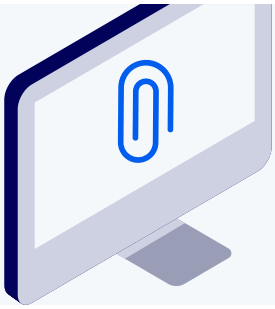
If a chargeback is raised against your business, we'll notify you by secure email. To view these messages, you will need to register your email address - here's how. You only need to do this once.

1



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

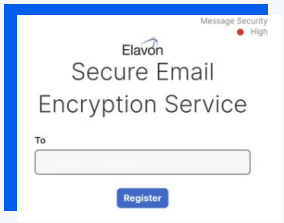
2



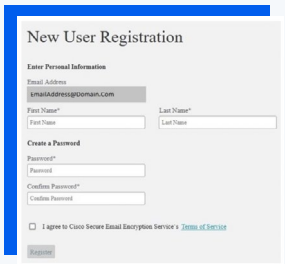
Click to **open the attachment** in your web browser.

3

Register your e-mail address with Cisco.

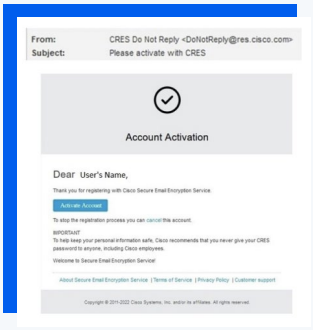


Complete each field in the form and click continue to submit. You should see a confirmation page



4

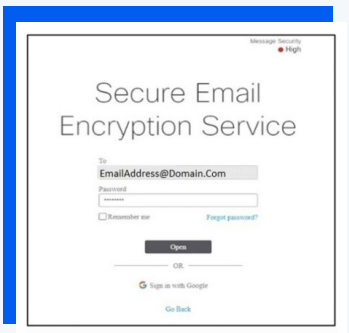
Check your email account for an email, with a button to **activate your account.**



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.**