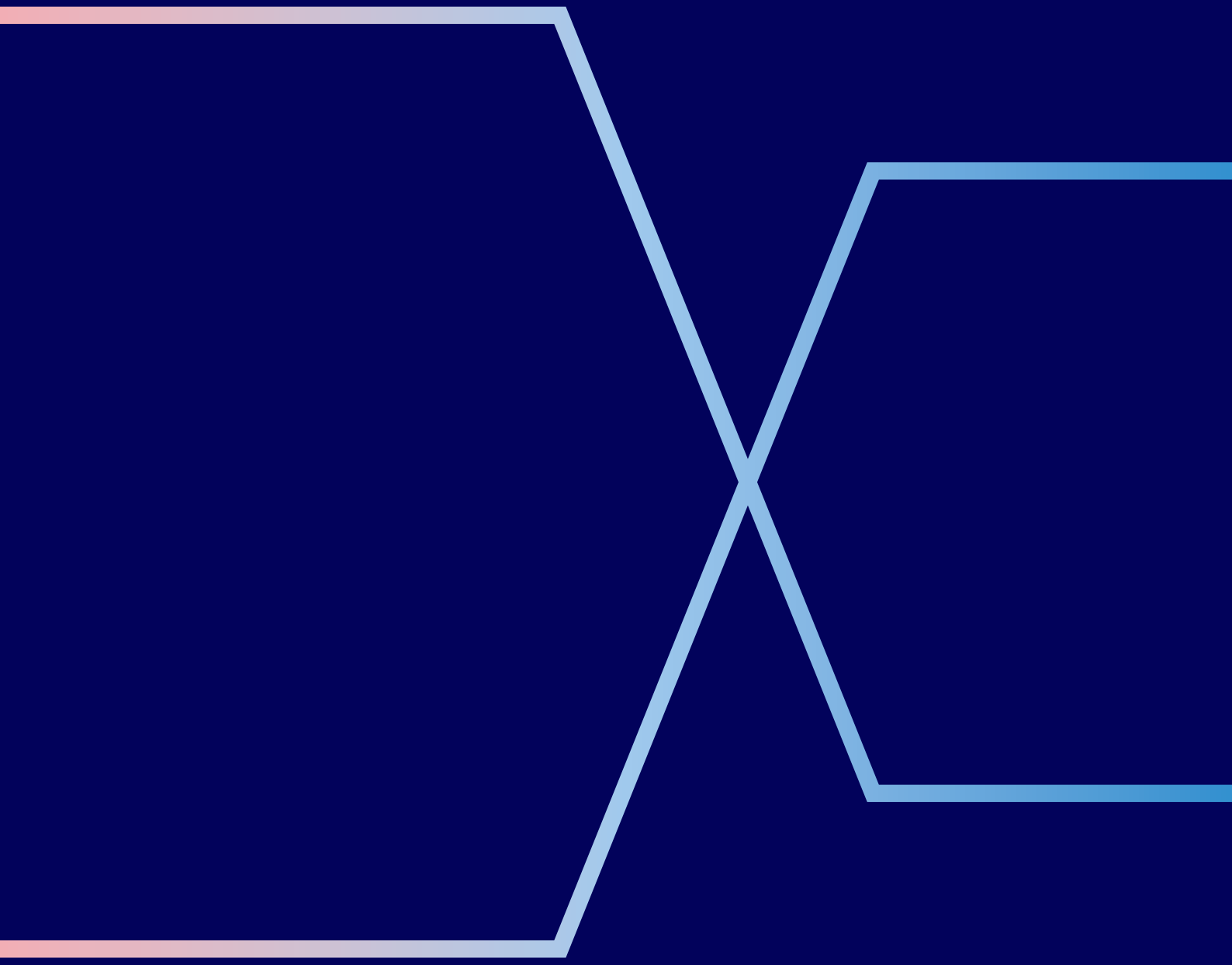
Beauty and medical services

Best practice for avoiding and managing chargebacks.



elavon®

This guide helps beauty salons, clinics, and wellness providers reduce chargebacks and respond effectively when disputes arise. It covers key areas from secure payments to client expectations and documentation. You can use it to train staff, create processes and minimise avoidable losses.

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 across all departments on how chargebacks work and their role in preventing them — reception, reservations, finance, etc.

Always refund to the original card. Avoid using cash, different cards, or bank transfers.

Never miss the response deadline — check “Respond By” dates, especially over bank holidays.

Don’t refund after a chargeback has been raised. Accept, defend or dispute, but avoid having to make double payments.

Keep your business name and address details updated to prevent disputes due to name mismatches or unrecognised transactions.

Use clear Terms & Conditions and refund policies:

In person: get a signature or print on the receipt.

- Over the phone/email: send written terms and get confirmation.
- Online: use a visible click-to-accept box with refund policy.
- Only submit files as PDFs or images, not cloud links (Google Drive, WeTransfer, etc.).

Prepare ready-to-use evidence packs including Ts & Cs, refund policy, signed consent forms, and before/after treatment info.

Fraud prevention

Use secure transaction methods.

- CHIP & PIN or contactless for in-person visits.
- 3D Secure for online or pay-by-link transactions.

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 and refusing the booking.

Encourage payments in person when clients arrive for appointments.

Use Code 10 and call the authorisation line for suspicious transactions or unusual client behaviour.

Watch out for friendly fraud, e.g. a family member claiming the service wasn’t authorised.

Verify the customer’s identity at check-in.

Don’t assume third-party bookings are safe — always confirm identity and cardholder consent at the time of service.

Never refund to a different card, even if a customer claims their card is lost or blocked. Ask them to raise a chargeback if needed.

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.

Follow terminal instructions — if referral is requested, call the number and input the code provided.

Avoid splitting payments to bypass limits.

Avoid pre-authorising debit cards (except minimal verification amounts), as they often lead to processing problems, and avoid using pre-authorisation with debit cards, unless verifying with a minimal amount (e.g. £0.01).

Complete pre-auths for exact amounts or use separate charges for extras like damage or minibar use. Avoid using codes older than 30 days.

Cancel declined or referral-requested transactions and process them properly after any necessary authorisation.

Don't use codes older than 30 days.

Processing errors

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

- "Void" or "Reversal" for if the transaction hasn't yet been settled.
- 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.

Provide itemised receipts for each transaction, clearly linking to the payment method and service.

Clearly explain currency and billing info on websites or in person to avoid misunderstandings.

Customer disputes

Keep detailed records of treatments, appointments, before/after photos, consent forms, and client messages.

Respond clearly to complaints — explain what the service involved, what the customer agreed to, and how the outcome was addressed.

Address client expectations early — provide realistic outcome explanations before cosmetic or
medical procedures.

Use signed waivers for non-refundable deposits or high-risk services.

Include full Ts & Cs and refund info when responding to chargebacks.

If a customer claims the product was counterfeit, provide invoices and supplier certifications.

Explain non-refunded cases properly:

- No-show for a non-refundable booking? Treat as “service not received” with policy evidence.
- Client unhappy with results but accepted correction or goodwill? Treat as “not as described” with documentation.

Keep copies of all correspondence, including texts, DMs, emails, and review site profiles and if complaints escalate, gather any external documentation to support your position.

Card transaction cycle

Customer chooses to **make a purchase**

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

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

Merchant sends payment data **requesting authorisation**

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

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

Merchant **gets paid**, minus any fees

Acquirer **deposits funds** into merchant account

Customer **receives purchase**

Chargeback transaction cycle

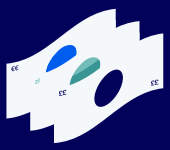
Customer **disputes a payment** with their bank

Issuing bank **pulls money back**

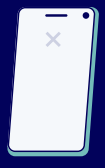
Card network **applies rules & deadlines**

Issuing bank **reviews decision**

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



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



Acquiring bank **passes claim** to merchant

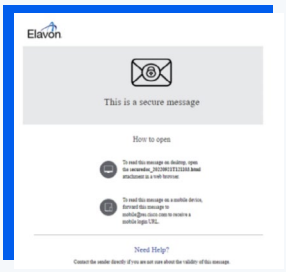
Merchant either: accepts **loss or** sends **evidence**

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

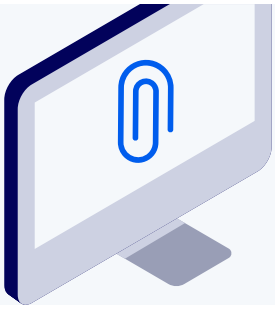
If a chargeback is raised against your business, we'll notify you by secure email. To view these messages, you will need to register your email address - here's how. You only need to do this once.

1



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

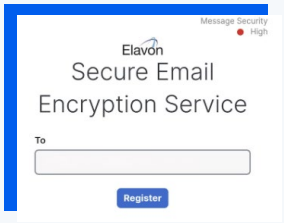
2



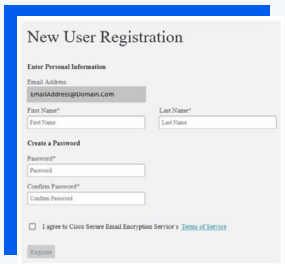
Click to **open the attachment** in your web browser.

3

Register your e-mail address with Cisco.

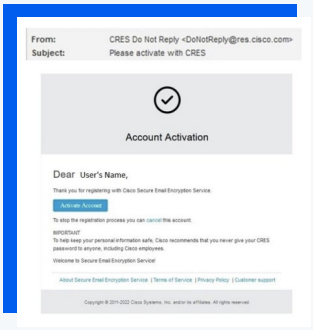


Complete each field in the form and click continue to submit. You should see a confirmation page



4

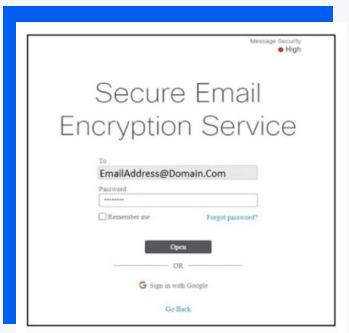
Check your email account for an email, with a button to **activate your account.**



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.**