What’s what in chargebacks?

An ABC glossary of terms.

elavon®

Acquirer

The financial institution or payments provider (like Elavon) that processes card payments on behalf of your business. Sometimes called your “merchant services provider."

Arbitration

The final step in a **chargeback** dispute when the card scheme (like Visa or Mastercard) makes a ruling. It can be costly and is best avoided with strong evidence upfront.

Authorisation code

The approval from a cardholder’s bank confirming that the transaction can go ahead. It checks that the card is valid and funds are available.

Cardholder

Your customer – the person who made the payment using their credit or debit card.

Card Scheme

The network that facilitates the card payment – e.g. Visa, Mastercard, or American Express. They set the rules and oversee the **chargeback** process.

Chargeback

A formal dispute where a customer (through their bank) asks for a card payment to be reversed. These are designed to protect customers but can affect your business if not handled well.

Elavon Connect

Our online customer portal where you can view and respond to chargebacks, receive alerts, and manage your account.

Issuer

The cardholder’s bank – they decide whether to approve transactions and whether to start a **chargeback.**

PCI-DSS

Short for Payment Card Industry Data Security Standard. A set of rules designed to keep card payments secure and protect customer data. All merchants must comply.

Reason Code

A code used to explain why a chargeback was raised. These fall into categories like fraud, processing errors, or customer disputes.

Retrieval Request

A request for documentation (like a receipt) before a **chargeback** is filed. Responding quickly can help avoid escalation.

What's the difference between secure and unsecure transactions?

Secure transactions

Secure transactions use **authentication and encryption** methods that confirm the cardholder's identity and protect card details. They're backed by fraud prevention measures and are easier to defend in **chargeback** cases.

What does it look like in practice?

Transaction type	What happens?	How it's secure?
Chip & PIN (in person)	Customer inserts their chip card and enters a PIN, which is validated.	PIN entry proves cardholder is there. Data is encrypted.
Contactless (NFC)	Customer taps card/device near the terminal. Limits apply	Uses tokenisation; transaction is encrypted.
3D Secure (online)	Customer is asked to verify their identity (e.g. SMS code, app, fingerprint).	Extra layer of authentication from cardholder's bank.
Digital Wallets (e.g. Apple Pay, Google Pay)	Customer uses biometrics or passcode to confirm.	Encrypted card details + secure authentication.

Magstripe cards

When a card is accepted by swiping the magnetic stripe on a card, the transaction carries extra risk and should be treated with caution.

What does it look like in practice?

Transaction type	What happens?	How it's secure?
Magstripe swipe (in-person)	Chip card is swiped and data from the magnetic stripe is read. No PIN is used.	Transaction should be madeas Chip & PIN. Liability shifts to merchant.
	Non-chip card is swiped and data from the magnetic stripe is read. No PIN is used.	Take extra care, but the transaction will be processed securely. Liability stays with bank.
	Card has been cloned to look like swipe card. Once swiped, transaction shown as manual entry.	This is a non-secure transaction.

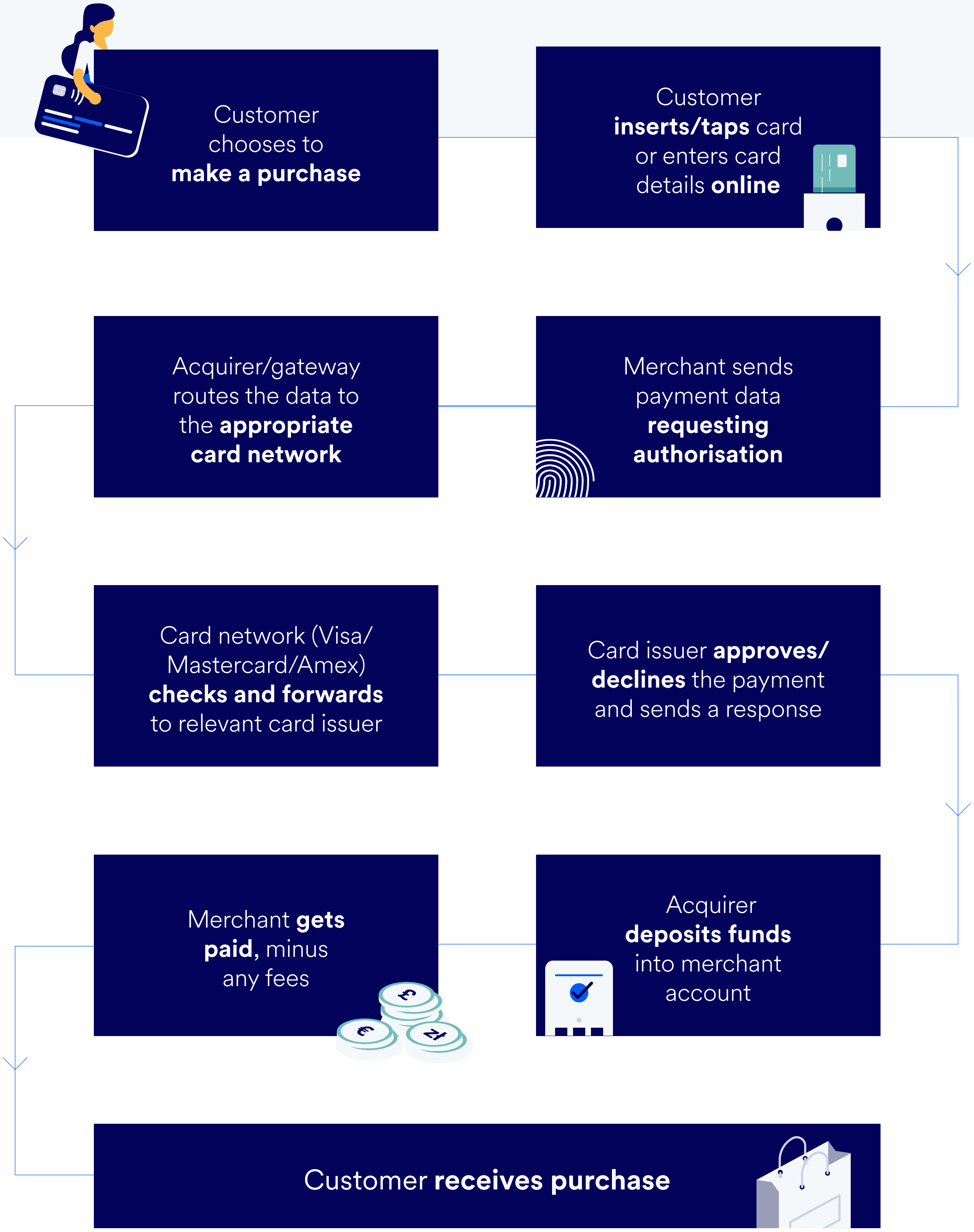
Unsecure Transactions

Unsecure transactions lack proper authentication or encryption, making them more vulnerable to fraud — and harder to defend if disputed.

What does it look like in practice?

Transaction type	What happens?	How it’s secure?
Manual key entry	Merchant manually types in the card number (e.g. over the phone).	No cardholder present. No authentication. High fraud risk.
Online checkout (no 3D Secure)	Customer enters card number, expiry and CVV only.	This is considered “card-not-present” and therefore unverified.
Offline transactions	Card accepted when terminal is offline. Can’t verify the transaction.	No real-time authorisation; transaction may later be declined.

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

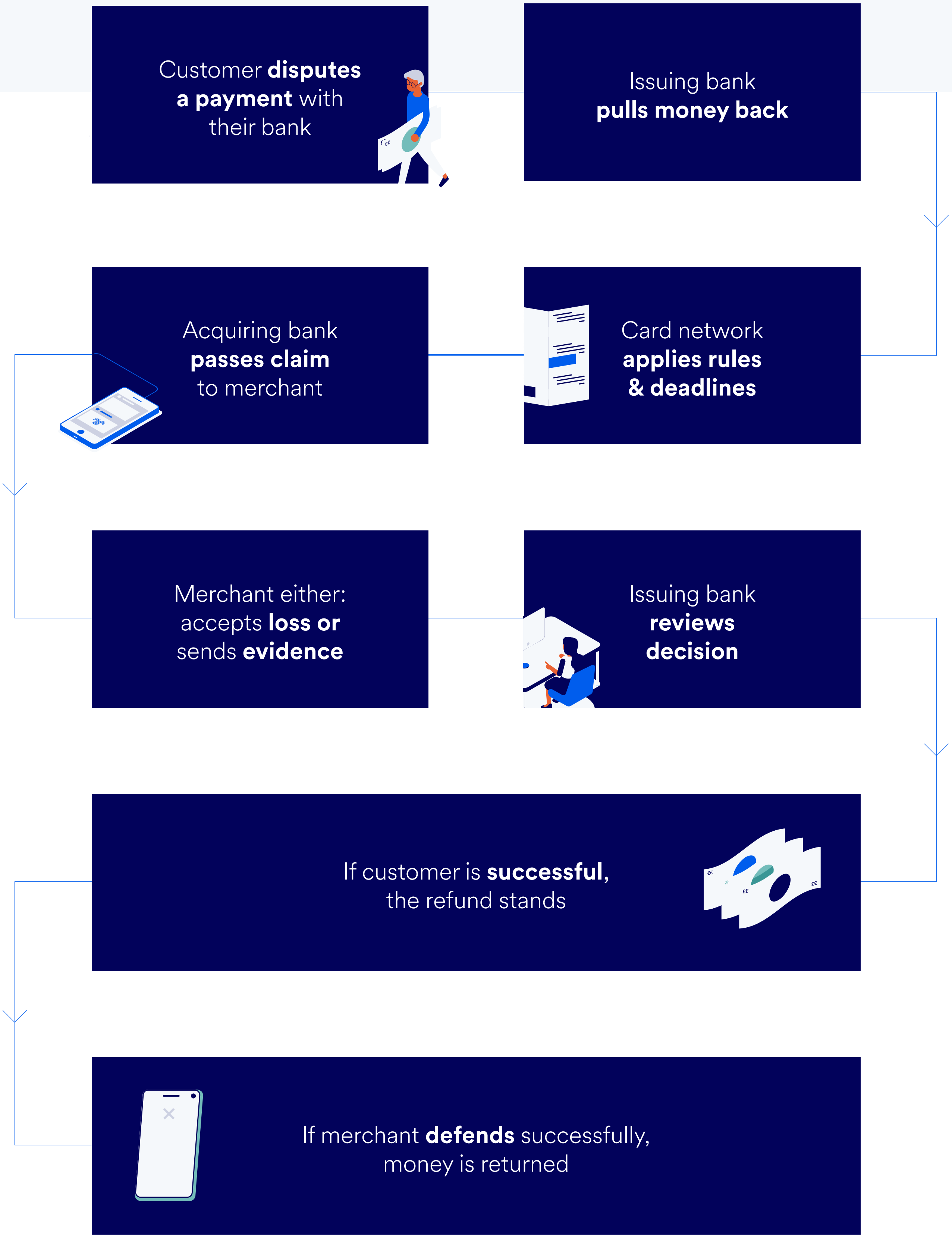
Card issuer **approves/ declines** the payment and sends a response

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**

Acquiring bank **passes claim** to merchant

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

Issuing bank **reviews decision**

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

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

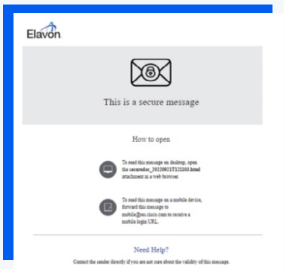
Contact us for more information

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


Elavon

This is a secure message

How to open

To read this message on desktop, open the securedoc_20220921T121103.html attachment in a web browser.

To read this message on a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

Need Help?

Contact the sender directly if you are not sure about the validity of this message.

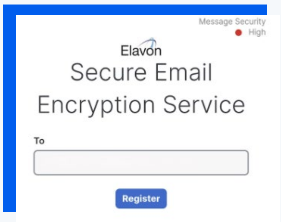
Look out for an email from **disputes@Elavon.com,** and save it to your device

2

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

3

Register your e-mail address with Cisco.

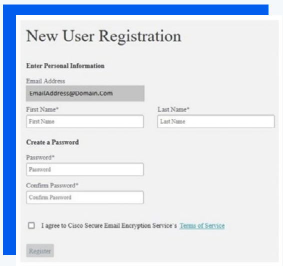

Message Security
● High

Elavon
Secure Email Encryption Service

To

Register

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


New User Registration

Enter Personal Information

Email Address: EmailAddress@Domain.Com

First Name*: First Name

Last Name*: Last Name

Create a Password

Password*: Password

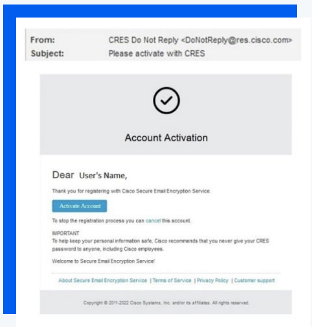
Confirm Password*: Confirm Password

☐ I agree to Cisco Secure Email Encryption Service`s Terms of Service

Register

4

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


From: CRES Do Not Reply <DoNotReply@res.cisco.com>
Subject: Please activate with CRES

Account Activation

Dear User's Name,

Thank you for registering with Cisco Secure Email Encryption Service.

Activate Account

To stop the registration process you can cancel this account.

IMPORTANT
To help keep your personal information safe, Cisco recommends that you never give your CRES password to anyone, including Cisco employees.

Welcome to Secure Email Encryption Service!

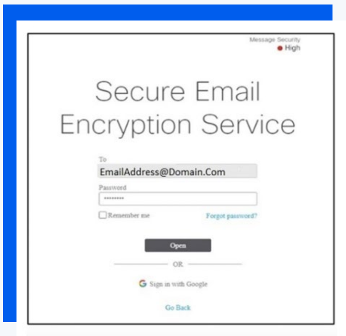
About Secure Email Encryption Service | Terms of Service | Privacy Policy | Customer support

Copyright © 2011-2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.


Message Security
● High

Secure Email Encryption Service

To: EmailAddress@Domain.Com

Password: *********

☐ Remember me Forgot password?

Open

OR

Sign in with Google

Go Back

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

U.S. Bank Europe DAC. Registered in Ireland – Number 418442. Registered Office: Block F1, Cherrywood Business Park, Dublin 18, D18 W2X7, Ireland.
U.S. Bank Europe DAC, trading as Elavon Merchant Services, is regulated by the Central Bank of Ireland.