# Merchant Operating Instructions

This documentation pack covers instructions and guidance for the smooth operation of your business when processing payments and refunds.

# Tyl by NatWest – Merchant Operating Instructions

## Contents


1. Purpose, Scope, and Audience ..... 7
   1.1 Purpose of this Manual ..... 7
   1.2 Scope of the Manual ..... 7
   1.3 Intended Audience ..... 8
2. How to Use This Manual ..... 8
   2.1 How the Manual Is Structured ..... 8
   2.2 Mandatory Requirements and Guidance ..... 9
   2.3 Keeping the Manual Up to Date ..... 9
3. Your Responsibilities as a Merchant ..... 10
   3.1 What It Means to Be a Merchant ..... 10
   3.2 General Merchant Responsibilities ..... 10
   3.3 Responsibility and Liability ..... 10
   3.4 Staff Training and Controls ..... 11
4. Payment Services Provided by Tyl by NatWest ..... 12
   4.1 Overview of Payment Services ..... 12
   4.2 Payment Channels ..... 12
   4.3 Importance of Using the Correct Payments Channel ..... 13
   4.4 Processing American Express Transactions ..... 13
5. Card Present Transactions (Face-to-Face Payments) ..... 14
   5.1 Definition of a Card Present Transaction ..... 14
   5.2 How Card Present Transactions Are Processed ..... 14
   5.3 Chip and PIN Cards ..... 14
   5.4 Contactless Payments ..... 15
      5.4.1 Contactless Cards ..... 15
      5.4.2 Digital Wallet Payments ..... 15

5.4.3 Good Practice for Contactless and Digital Wallet Payments ..... 16
5.5 Receipts and Records ..... 16
5.6 Risk Considerations for Card Present Transactions ..... 16
6. Card Not Present Transactions ..... 17
6.1 Definition of a Card Not Present Transaction ..... 17
6.2 Channels Used for Card Not Present Transactions ..... 17
6.3 Information You Must Collect ..... 17
6.4 Fraud Risk and Liability ..... 18
6.5 Operational Best Practice ..... 18
7. Online Payments ..... 19
7.1 What Are Online Payments? ..... 19
7.2 Checkout Payment pages ..... 19
7.3 Hosting your own Checkout Payment Pages ..... 19
7.4. Pay by Link and Virtual Terminal Payments ..... 20
7.4.1 What Is Pay by Link? ..... 20
7.4.2 Virtual Terminal Payments ..... 20
7.4.3 Risks and Controls ..... 20
7.4 Declined Online Transactions ..... 20
8. Authorisation and Transaction Types ..... 21
8.1 What Is Authorisation? ..... 21
8.2 Sale Transactions ..... 21
8.3 Authorisation-Only Transactions ..... 21
8.4 Pre-Authorisation and Completion ..... 22
8.5. Deferred, Recurring, and Ongoing Transactions ..... 22
8.5.1 Deferred Supply Transactions ..... 22
8.5.2 Recurring Transactions ..... 22
8.6. Merchant Initiated Transactions ..... 24
8.6.1 What Is a Merchant Initiated Transaction? ..... 24
8.6.2 Requirements for Merchant Initiated Transactions ..... 24
8.6.3 Risk Considerations ..... 24
9. The Transaction Lifecycle ..... 25

9.1 Overview of the Transaction Lifecycle ..... 25
9.2 Transaction Initiation ..... 25
9.3 Authorisation Stage ..... 25
9.4 Clearing Stage ..... 26
9.5 Settlement Stage (Referred to as Payouts in the Customer Portal) ..... 26
10. Settlement, Payouts, and Reconciliation ..... 27
10.1 What Is Settlement? ..... 27
10.2 Payout Timing ..... 27
10.3 Gross and Net Settlement ..... 27
10.4 Reconciling Transactions ..... 27
11. Refunds, Reversals, and Noncompliant Refunds ..... 28
11.1 What Is a Refund? ..... 28
11.2 What Is a Reversal or Void? ..... 28
11.3 Non-Compliant Refunds ..... 28
11.4 Merchant Responsibilities for Refunds ..... 28
12. Chargebacks and Disputes ..... 29
12.1 What Is a Chargeback? ..... 29
12.2 Common Reasons for Chargebacks ..... 29
12.3 Your Role in a Chargeback ..... 29
12.4 Timeframes and Deadlines ..... 30
12.5. Chargeback Evidence and Outcomes ..... 30
12.5.1 What Is Chargeback Evidence? ..... 30
12.5.2 Providing Effective Evidence ..... 30
12.5.3 Chargeback Outcomes ..... 31
12.6 Monitoring Chargeback Levels ..... 31
13. Fraud Risk and Fraud Reduction ..... 32
13.1 What Is Payment Fraud? ..... 32
13.2 Fraud Risk by Payment Channel ..... 32
13.3 Your Responsibilities in Reducing Fraud ..... 32
13.4 Indicators of Potential Fraud ..... 32
13.4.1 Passwords ..... 33
13.5. Strong Customer Authentication and 3D Secure ..... 33

13.5.1 What Is Strong Customer Authentication? ..... 33
13.5.2 How Strong Customer Authentication Works ..... 33
13.5.3 What Is 3D Secure? ..... 33
13.5.4 Impact on Liability ..... 34
14. Data Security and PCI DSS Compliance ..... 34
14.1 Protecting Payment Data ..... 34
14.2 What Is PCI DSS? ..... 34
14.3 Your PCI DSS Responsibilities ..... 34
14.4 Consequences of Non-Compliance ..... 35
15. Record Keeping and Transaction Retention ..... 35
15.1 Why Record Keeping Is Important ..... 35
15.2 Types of Records You Must Keep ..... 35
15.3 Retention Periods ..... 36
15.4 Secure Storage of Records ..... 36
16. Staff Access, Training, and Internal Controls ..... 37
16.1 Managing Staff Access ..... 37
16.2 Staff Training Requirements ..... 37
16.3 Internal Controls ..... 37
17. Prohibited and Restricted Activities ..... 38
17.1 Understanding Prohibited Transactions ..... 38
17.2 Examples of Prohibited Activities ..... 38
17.3 Your Responsibility to Comply ..... 40
18. Account Changes, Updates, and Notifications ..... 40
18.1 Why You Must Notify Changes ..... 40
18.2 How Changes May Impact Your Account ..... 40
18.3 Keeping Contact Details Accurate ..... 40
19. Service Issues, Declines, and Troubleshooting ..... 42
19.1 Understanding Transaction Declines ..... 42
19.2 What to Do When a Transaction Is Declined ..... 42
19.3 Service Interruptions ..... 42
19.4 Getting Support ..... 42
20. Fees, Invoicing, and Statements ..... 43

20.1 Understanding Fees ..... 43
20.2 Invoices ..... 43
20.2.1 Reviewing invoices ..... 43
20.3 Direct Debits and Fee Collection ..... 44
21. Complaints and Escalation ..... 45
21.1 Raising a Complaint ..... 45
21.2 Complaint Handling Process ..... 45
21.3 Escalating a Complaint ..... 45
22. Suspension and Termination of Services ..... 46
22.1 When Services May Be Suspended ..... 46
22.2 Termination of Services ..... 46
22.3 Your Responsibilities Following Termination ..... 46
23 Legal and Regulatory Framework ..... 47
23.1 Applicable Laws and Regulations ..... 47
23.2 Data Protection Obligations ..... 47
23.3 Regulatory Changes ..... 47
24. Glossary of Terms ..... 48
25. Frequently Asked Questions (FAQs) ..... 49
25.1 Account Access and User Management ..... 49
25.2 Transactions and Reporting ..... 49
25.3 Payment Links ..... 50
25.4 Refunds ..... 51
25.5 Payit (Open Banking Payments) ..... 52
25.6 Support and Troubleshooting ..... 54

# 1. Purpose, Scope, and Audience

## 1.1 Purpose of this Manual

This Merchant Operating Manual explains how merchants can accept payments for goods and services using **Tyl by NatWest**. It sets out the rules, responsibilities, and processes you should follow to take payments securely, accurately, and in line with industry and regulatory requirements.

**The manual has four main purposes:**

1. To explain how Tyl by NatWest payment services work in practice
2. To support you in processing payments correctly across different payment channels
3. To reduce the risk of fraud, disputes, and chargebacks
4. To help you meet your contractual, regulatory, and data-protection obligations

This document is written for merchants; it avoids unnecessary legal language where possible and focuses on practical guidance.

You should read this manual alongside your **Merchant Services Agreement** and any product-specific terms you have agreed to. Where there is a difference between documents, your Merchant Services Agreement takes precedence.

## 1.2 Scope of the Manual

This manual applies to **all merchants** who use Tyl by NatWest to accept payments, regardless of:

- Business size
- Industry sector
- Payment methods or channels used

**It covers the full lifecycle of a payment, including:**

- Accepting payments from customers
- Authorising and processing transactions
- Receiving settlement and payouts
- Issuing refunds
- Managing disputes and chargebacks

- Preventing fraud and protecting data

All guidance in this manual applies to transactions processed through Tyl by NatWest unless stated otherwise.

### 1.3 Intended Audience

**This manual is intended for:**

- Business owners and company directors
- Store managers and operational managers
- Customer service teams
- Any employees involved in taking, refunding, or managing payments

You do not need specialist payments knowledge to use this manual. Where technical terms are used, they are explained when first introduced.

## 2. How to Use This Manual

### 2.1 How the Manual Is Structured

This manual is structured to follow the **natural journey of a payment** from the point a customer chooses to pay through to settlement, reconciliation, and, where relevant, refunds or disputes.

The sections are grouped broadly as follows:

1. **Foundations** – explanations of services, responsibilities, and key concepts
2. **Payment acceptance** – how to take payments across different channels
3. **Transaction processing** – authorisation, clearing, and settlement
4. **After the payment** – refunds, chargebacks, and dispute handling
5. **Risk and compliance** – fraud prevention, security, and data protection
6. **Account management** – changes, support, and ongoing obligations

You should read this manual before taking payments and keep it as a reference when questions or issues arise.

## 2.2 Mandatory Requirements and Guidance

**Throughout this document:**

- Statements describing actions you **must** take are mandatory requirements
- Explanatory or advisory statements provide guidance and best practice

**Mandatory requirements are based on:**

- Card scheme rules (for example, Visa, Mastercard, and American Express rules)
- Regulatory requirements
- Your Merchant Services Agreement (MSA) with Tyl by NatWest

**Failure to follow mandatory requirements may result in:**

- Financial losses
- Customer disputes
- Chargebacks
- Additional monitoring or restrictions on your account

## 2.3 Keeping the Manual Up to Date

Payment rules and regulations can change. We'll update this manual as needed to reflect:

- Changes to card scheme rules
- Regulatory updates
- New payment products or features

You're responsible for ensuring that you and your staff follow the most recent version.

# 3. Your Responsibilities as a Merchant

## 3.1 What It Means to Be a Merchant

When you use Tyl by NatWest to accept payments, you become a **merchant**. A merchant is a business that accepts payment cards or other electronic payment methods in exchange for goods or services.

As a merchant, you're responsible for how payments are taken, processed, and managed within your business. While Tyl by NatWest provides payment services and infrastructure, this does not remove your responsibilities.

## 3.2 General Merchant Responsibilities

You're responsible for ensuring that:

- Only genuine transactions are processed
- Transactions are processed accurately and for the correct amounts
- Payments are taken using approved methods and channels
- Customer data is protected
- Staff follow correct procedures

These responsibilities apply when a payment is taken using the following approved channels:

- In person
- Online
- Over the phone
- Using a payment link

## 3.3 Responsibility and Liability

The level of financial risk you carry depends on how a transaction is processed. In general:

- Transactions where the customer and their payment card are physically present tend to carry lower fraud risk
- Transactions where the card is not physically presented tend to carry higher fraud risk

Later sections of this manual explain how processing methods affect liability in more detail.

## 3.4 Staff Training and Controls

Make sure that:

- Staff involved in payment processing are trained
- Access to payment systems is restricted to authorised staff
- Payment equipment and login details are kept secure
- Procedures are followed consistently

Errors made by staff are treated as merchant errors and remain your responsibility.

# 4. Payment Services Provided by Tyl by NatWest

## 4.1 Overview of Payment Services

Tyl by NatWest provides services that allow you to accept electronic payments from customers.

**These services include:**

- Card payments using debit and credit cards (Visa Mastercard, American Express and Diners Discover)
- Contactless payments (Visa Mastercard, American Express and Diners Discover)
- Digital wallet payments, such as Apple Pay and Google Pay
- Online payments through checkout payment pages or application programming interfaces (APIs) (Visa Mastercard, American Express and Diners Discover)
- Telephone and mail order payments (Visa Mastercard, American Express and Diners Discover)
- Payment links (Visa Mastercard, American Express and Diners Discover)
- Open Banking payments using Payit

Each service uses the same core payment infrastructure but has different operating requirements and risk profiles.

**For transactions, Tyl supports GBP (British Pound) currency only.**

## 4.2 Payment Channels

A **payment channel** is the way a payment is accepted. Common payment channels include:

- Payments taken in person using a card machine
- Payments taken online through a website
- Payments taken over the phone
- Payments taken via a secure payment link using the Virtual Terminal

You must only use payment channels that have been approved and enabled on your account.

## 4.3 Importance of Using the Correct Payments Channel

Each payment channel is governed by specific rules. Using the wrong channel can:

- Increase fraud risk
- Invalidate transaction protections
- Result in chargebacks
- Breach your agreement

For example, a payment taken over the phone must not be processed as if the customer were physically present.

## 4.4 Processing American Express Transactions

Tyl by NatWest supports American Express (Amex) payments across card machines, online, and phone transactions.

Businesses can accept Amex alongside Visa and Mastercard, but it must be specifically requested during onboarding or added later, as it requires separate setup.

Fees for Amex processing vary by industry and are provided by sales or customer service.

Amex acceptance is available in most cases, though some specific scenarios (such as charity donations via physical terminals) may be excluded and should be discussed with Tyl.

# 5. Card Present Transactions (Face-to-Face Payments)

## 5.1 Definition of a Card Present Transaction

A **card present transaction** is a transaction where:

- The customer is physically present at the point of sale
- The customer presents their payment card in person
- The transaction is processed using a card machine

Card present transactions use the security features built into payment cards and card machines, which helps to reduce fraud risk when processed correctly.

Guides to card machines can be found on Tyl's help and support section.

## 5.2 How Card Present Transactions Are Processed

For a card present transaction:

1. The total amount is entered into the card machine
2. The customer inserts or taps their card
3. The card machine communicates with the card issuer to request approval
4. The customer enters their personal identification number (PIN) if required
5. The transaction is approved or declined

You must follow all on-screen prompts shown on the card machine.

## 5.3 Chip and PIN Cards

Most payment cards contain an embedded computer chip. When a card is inserted into the card machine, the chip is used to:

- Confirm the card is genuine
- Create a secure, one-time transaction record

The customer enters a personal identification number (**PIN**), which is known only to them and their card issuer. This provides strong confirmation that the customer is authorised to use the card.

## 5.4 Contactless Payments

A **contactless payment** is a type of card present transaction where the customer does not insert their card into the card machine. Instead, the customer taps their card or device against the card machine to complete a payment.

Contactless payments rely on short-range wireless communication between the card or device and the card machine. This allows payments to be completed quickly and conveniently.

Contactless payments are subject to transaction limits and security controls set by card issuers and card schemes.

**Card issuers may still request a PIN:**

- After a number of contactless payments
- Once a cumulative spending limit is reached

**You must not attempt to override these checks.**

### 5.4.1 Contactless Cards

A **contactless card** is a debit or credit card enabled with contactless technology. These cards display a contactless symbol and can be used by tapping them against a compatible card machine.

For lower value transactions, the customer is usually not required to enter a personal identification number (PIN). However, the card issuer may require PIN entry:

- After a certain number of contactless transactions
- Once a cumulative spending threshold has been reached
- When the transaction is considered higher risk

You must always follow the instructions displayed on the card machine.

### 5.4.2 Digital Wallet Payments

A **digital wallet** allows a customer to store their card details securely on a mobile phone, smartwatch, or other supported device. Common digital wallets include Apple Pay and Google Pay.

**When a customer pays using a digital wallet:**

- The device generates a secure payment credential
- The customer may be required to authenticate using biometrics or a device passcode

- The transaction is processed as a contactless card-present payment

From an operational perspective, digital wallet payments are treated similarly to contactless card payments, but with additional security features.

#### 5.4.2.1 Security and Liability for Contactless and Digital Wallet Payments

Digital wallets use advanced security controls, such as encryption and device authentication. This can reduce fraud risk compared to traditional card use.

**However, you must still:**

- Process the payment using a compatible card machine
- Follow all terminal prompts
- Ensure the transaction amount is correct

Failing to follow correct procedures may affect liability if a transaction is disputed.

### 5.4.3 Good Practice for Contactless and Digital Wallet Payments

**To reduce risk, you should:**

- Ensure card machines are kept secure and regularly inspected
- Be alert to unusual customer behaviour
- Never attempt to bypass security checks
- Always allow the card machine to control whether PIN entry is required

## 5.5 Receipts and Records

You should always offer a receipt to the customer. Transaction records may be needed later for:

- Customer queries
- Refunds
- Chargeback responses

Records must be stored securely.

## 5.6 Risk Considerations for Card Present Transactions

Although card present transactions are generally lower risk, fraud can still occur. You should be alert to:

- Damage or unusual features on a card

- Behaviour that suggests the customer may not be authorised
- Attempts to rush staff or avoid verification steps

If something does not seem right, you should pause the transaction and follow your internal procedures.

# 6. Card Not Present Transactions

## 6.1 Definition of a Card Not Present Transaction

A **card-not-present transaction** is a payment where:

- The customer is not physically present at the point of sale, and
- The payment card is not physically presented to you

**Card Not Present transactions include payments taken:**

- Through a website
- Over the phone
- By mail order
- Via a secure payment link sent via Text, WhatsApp, or email.

Because the card and cardholder are not physically verified, card not present transactions typically carry a higher risk of fraud.

## 6.2 Channels Used for Card Not Present Transactions

**Card not present transactions can be processed through the following channels:**

- Online through a website
- A virtual terminal accessed through a secure portal
- Pay by Link
- Application-based integrations provided by Tyl by NatWest (API)

Each channel has specific operating rules, but all card-not-present transactions share similar risk characteristics.

## 6.3 Information You Must Collect

When processing a card-not-present transaction, you must collect certain information from the customer. This typically includes:

- The card number

- The card expiry date
- The cardholder's name
- The card security code (also known as CVV or CVC)
- The billing address associated with the card

This information is used to carry out verification checks and request authorisation from the card issuer.

You must not store the card security code after authorisation.

## 6.4 Fraud Risk and Liability

**For card-not-present transactions:**

- **Fraud liability usually rests with the merchant**
- Authorisation alone does not guarantee protection against fraud
- Additional security measures may reduce liability in certain circumstances

Later sections explain how additional authentication affects liability.

## 6.5 Operational Best Practice

**To reduce the risk of disputes and fraud for card-not-present transactions, you should:**

- Use the approved Tyl by NatWest channels
- Ensure billing information is entered accurately
- Only dispatch goods after confirmation of authorisation
- Keep records of customer communications and delivery

# 7. Online Payments

## 7.1 What Are Online Payments?

An **online payment** is a card-not-present transaction where a customer enters their payment details into a payment page through a website or application.

**Online payments are commonly used for:**

- E-commerce purchases
- Service bookings
- Digital products
- Invoices paid electronically

## 7.2 Checkout Payment pages

A **checkout payment page** is a payment page provided by Tyl by NatWest where:

- The customer is redirected to a secure page
- Payment details are entered directly into Tyl by NatWest systems
- The merchant does not handle or store card details

Checkout payment pages help reduce your data security burden as Tyl host the payment page and collect and/or store payment information on the merchant's behalf.

Please follow this link to the latest checkout payment page integration guide

## 7.3 Hosting your own Checkout Payment Pages

You can choose to host your own checkout payment page and use Tyl's API to submit payment requests. If you do, there are a few important things to be aware of:

- You're responsible for how payment data is captured and managed
- You'll need to meet additional security and compliance requirements
- Your systems must meet PCI DSS standards
- You'll need to implement 3D Secure (3DS)

If you decide to host your own checkout payment page, it's important that you understand and meet these requirements in full.

## 7.4. Pay by Link and Virtual Terminal Payments

### 7.4.1 What Is Pay by Link?

**Pay by Link** allows you to generate a secure payment link and send it to a customer using:

- Email
- Text message
- Messaging applications

When the customer clicks the link, they are taken to a secure payment page to complete the payment.

### 7.4.2 Virtual Terminal Payments

A **virtual terminal** is a secure online portal that allows you to enter card details manually to process a payment. Virtual terminals are commonly used for:

- Telephone payments
- Mail-order payments
- One-off card-not-present transactions

Access to the virtual terminal must be restricted to authorised and trained staff.

Please follow this link to the latest Virtual Terminal User guide.

### 7.4.3 Risks and Controls

Both Pay by Link and virtual terminal payments are card-not-present transactions and carry higher fraud risk.

**You should:**

- Verify customer information carefully
- Keep detailed transaction records
- Ensure payment links are managed securely
- Never request card details through insecure channels

## 7.4 Declined Online Transactions

Online transactions may be declined for many reasons, including:

- Insufficient funds
- Incorrect card details

- Issuer fraud checks
- Regulatory requirements

If a transaction is declined, you should advise the customer to contact their card issuer.

# 8. Authorisation and Transaction Types

## 8.1 What Is Authorisation?

**Authorisation** is the process by which a transaction request is sent to the cardholder's bank (known as the card issuer) to confirm that:

- The card is valid
- Funds or credit are available

Authorisation does not guarantee settlement, but it is required before completing a transaction.

**Using the incorrect transaction type can lead to:**

- Declined payments
- Customer complaints
- Chargebacks
- Additional fees

Make sure that you understand and use the correct transaction type for your business.

## 8.2 Sale Transactions

A **sale transaction** is the most common type of transaction. In a sale:

- The transaction is authorised
- The amount is captured for settlement
- Funds move through the payment process automatically

## 8.3 Authorisation-Only Transactions

An **authorisation-only transaction** places a temporary hold on funds but does not immediately capture them for settlement.

**You must:**

- Complete the transaction within the allowed time period
- Capture the correct amount
- Release unused authorisations promptly

## 8.4 Pre-Authorisation and Completion

A **pre-authorisation** is used where the final transaction amount is not known at the time of payment, such as in hospitality or vehicle hire.

Once the final amount is known, the transaction must be completed by capturing the authorised amount.

## 8.5. Deferred, Recurring, and Ongoing Transactions

### 8.5.1 Deferred Supply Transactions

A **deferred supply transaction** occurs when a customer pays for goods or services that are delivered at a later date. Common examples include:

- Advance bookings
- Pre-orders
- Services provided at a future time

In these cases, there is a time gap between when the payment is taken and when the customer receives the goods or services.

**When you accept payment for a deferred supply:**

- You must clearly explain delivery timelines to the customer
- You must provide a refund if goods or services cannot be delivered as agreed
- You must comply with consumer protection requirements

If delivery is delayed beyond what was agreed, customers may raise disputes with their card issuer.

### 8.5.2 Recurring Transactions

A **recurring transaction** is a payment that is taken automatically at regular intervals, such as weekly, monthly, or annually. Recurring transactions are often used for:

- Subscriptions
- Membership fees

- Instalment plans

Recurring transactions require **advance customer agreement**.

**Before processing recurring transactions, make sure you ensure that:**

- The customer has clearly agreed to recurring payments
- The amount and frequency are disclosed
- The customer understands how to cancel

#### 8.5.2.1 Customer Consent for Ongoing Payments

**Customer consent must be obtained before the first payment is taken. Consent may be collected:**

- Online
- In writing
- Through recorded verbal agreement

You're responsible for retaining evidence of consent. This evidence may be required if a payment is disputed.

**Customers must be given clear information about:**

- When payments will be taken
- How much will be taken
- How payments can be cancelled

#### 8.5.2.2 Changes to Recurring Payments

If you make changes to the amount or timing of a recurring payment, you must:

- Notify the customer in advance
- Allow the customer to cancel if they do not agree
- Provide reasonable notice of changes

Failure to manage changes correctly may result in disputes or chargebacks.

## 8.6. Merchant Initiated Transactions

### 8.6.1 What Is a Merchant Initiated Transaction?

A **merchant-initiated transaction (MIT)** is a payment taken without the customer actively participating at the time the payment is processed.

**Merchant initiated transactions are typically used for:**

- Subscription renewals
- Outstanding balances
- No-show charges
- Additional agreed charges

These transactions can only take place if the customer has previously given permission.

### 8.6.2 Requirements for Merchant Initiated Transactions

**Before processing a merchant-initiated transaction:**

- An initial customer-initiated transaction must have been completed
- The customer must have provided clear permission
- The payment must relate to the original agreement

**You must be able to show evidence that:**

- The customer agreed to future charges
- The customer was informed of cancellation options

If these requirements are not met, the transaction is likely to be disputed. A 14-day notice period must be given for any changes to the amount or the date the transaction is processed, changes and cancellation procedures.

MITs are available on Card Not Present transactions only.

### 8.6.3 Risk Considerations

Merchant initiated transactions carry increased risk because the customer is not actively involved at the time of payment.

**To reduce risk, you should:**

- Communicate clearly with customers

- Use clear billing descriptions
- Send reminders before charges where possible
- Maintain accurate records for future reference to support any customer, compliance or regulatory queries.

# 9. The Transaction Lifecycle

## 9.1 Overview of the Transaction Lifecycle

Every payment follows a series of steps known as the **transaction lifecycle**. Understanding this lifecycle helps you:

- Identify where issues may occur
- Respond effectively to customer queries
- Reconcile payments and settlements

**The transaction lifecycle includes:**

1. Transaction initiation
2. Authorisation
3. Clearing
4. Settlement

Each stage serves a different purpose.

## 9.2 Transaction Initiation

A transaction starts when a customer tries to make a payment. This may happen:

- At a card machine
- On a website
- Via a payment link
- Over the phone

At this stage, payment details are captured and prepared for authorisation.

## 9.3 Authorisation Stage

Authorisation occurs when the transaction request is sent to the card issuer. The issuer checks:

- Whether the card is valid

- Whether funds or credit are available
- Whether the transaction appears suspicious

The transaction may be approved or declined.

## 9.4 Clearing Stage

Clearing is the process of submitting approved transactions into the payment system so that funds can be transferred.

**Transactions are usually cleared:**

- At the end of the business day
- In batches

If transactions are not submitted within required timeframes, they may be declined or reversed.

## 9.5 Settlement Stage (Referred to as Payouts in the Customer Portal)

Settlement is the stage where funds are transferred from the card issuer to the acquiring bank and then paid into your nominated bank account.

**Settlement timing depends on:**

- The payment method
- The day the transaction occurred
- Any reviews or delays

# 10. Settlement, Payouts, and Reconciliation

## 10.1 What Is Settlement?

**Settlement** refers to the movement of funds from completed transactions into your bank account. Settlement does not usually happen instantly.

**Most card payments are settled:**

- On the next business day
- After all required checks are completed

## 10.2 Payout Timing

**Payout timing may vary due to:**

- Weekends and bank holidays
- Transaction reviews
- Outstanding disputes or refunds

You should not assume that settlement is guaranteed on a specific day.

## 10.3 Gross and Net Settlement

**Merchants may receive settlements:**

- **Gross**: where fees are charged separately
- **Net**: where fees are deducted before funds are paid out

Your settlement method is set as part of your agreement.

## 10.4 Reconciling Transactions

**You should regularly reconcile:**

- Transactions taken
- Funds received
- Fees charged

**Reconciliation helps identify:**

- Missing payments
- Duplicate entries
- Processing errors

# 11. Refunds, Reversals, and Noncompliant Refunds

## 11.1 What Is a Refund?

**A refund is the return of funds to a customer after a completed transaction. Refunds must:**

- Be issued to the original payment method
- Reference the original transaction
- Refunds must be processed promptly. In most cases, you should submit refunds as soon as you're aware they're needed.
- Cash refunds for card payments are not permitted.

## 11.2 What Is a Reversal or Void?

A **reversal**, also known as a void, cancels a transaction before it has been settled.

Reversals are time-sensitive. Once a transaction has settled, it must be refunded instead.

## 11.3 Non-Compliant Refunds

**A refund may be considered non-compliant if:**

- It is issued to a different card or account
- It is processed incorrectly as a new sale
- Required authorisation is not obtained
- It is submitted outside allowed timeframes

Non-compliant refunds increase the risk of disputes and penalties.

## 11.4 Merchant Responsibilities for Refunds

**You're responsible for:**

- Processing refunds correctly
- Ensuring you have sufficient funds
- Communicating with customers
- Retaining refund records

Incorrect refund handling is a common cause of chargebacks.

Please follow the guide for the specific Terminal you have in our help and support section here.

# 12. Chargebacks and Disputes

## 12.1 What Is a Chargeback?

A **chargeback** occurs when a customer contacts their card issuer (their bank) to dispute a card transaction and requests that the funds be returned. This is different from a refund, which is initiated by you directly.

Chargebacks exist to protect customers, but we know they can be time-consuming and costly for merchants to deal with.

**A chargeback process typically involves:**

- The customer raising a dispute with their card issuer
- The issuer temporarily reclaiming the transaction value
- The merchant being asked to provide information or evidence
- A final decision being made by the card issuer

## 12.2 Common Reasons for Chargebacks

**Chargebacks are usually raised for one of the following reasons:**

- The customer does not recognise the transaction
- The goods were not received
- The goods or services were not as described
- A refund was expected but not processed
- The card was used without authorisation

Many disputes arise not from fraud, but from **misunderstanding, poor communication, or processing errors**.

## 12.3 Your Role in a Chargeback

**When a chargeback is raised:**

- Tyl by NatWest is notified by the card scheme
- We'll inform you and ask you to provide information
- You must respond within the stated timeframe

If you do not respond on time, the chargeback will usually be decided in the customer's favour automatically.

**You remain responsible for:**

- Providing accurate evidence
- Ensuring evidence is submitted on time
- Accepting the outcome decided by the issuer

## 12.4 Timeframes and Deadlines

**Chargeback deadlines are strict. You must:**

- Review notifications promptly
- Gather requested information quickly
- You must respond within the stated timeframe, which is often a matter of days rather than weeks.
- Failure to meet deadlines almost always results in a loss of the dispute.

## 12.5. Chargeback Evidence and Outcomes

### 12.5.1 What Is Chargeback Evidence?

**Chargeback evidence** (sometimes called compelling evidence) is documentation that supports your position that a transaction is valid.

**Common examples include:**

- Proof of delivery
- Signed receipts (where applicable)
- Transaction logs
- Customer correspondence
- Evidence of customer consent

The type of evidence required depends on the reason the customer raised the dispute.

### 12.5.2 Providing Effective Evidence

**To maximise your chances of success:**

- Ensure evidence is clear and legible
- Provide only relevant information

- Ensure customer information matches the disputed transaction
- Avoid submitting unnecessary or unrelated documents

Submitting incomplete or inaccurate evidence reduces the likelihood of a favourable outcome.

### 12.5.3 Chargeback Outcomes

**After reviewing the evidence:**

- The card issuer decides whether the chargeback is upheld or reversed
- If upheld, the customer keeps the refunded funds
- If reversed, the funds may be returned to you

The card issuer's decision is final.

Even if a chargeback is reversed, a fee may still apply.

## 12.6 Monitoring Chargeback Levels

**Consistently high chargeback levels may indicate issues with:**

- Fraud controls
- Customer communication
- Refund handling

**High chargeback ratios can result in:**

- Additional monitoring
- Increased fees
- Restrictions on your account
- Termination of services in serious cases

# 13. Fraud Risk and Fraud Reduction

## 13.1 What Is Payment Fraud?

**Payment fraud** occurs when a transaction is carried out using a card or payment method without the cardholder's authorisation.

**Fraud can affect:**

- Card-present transactions
- Card-not-present transactions
- Recurring or merchant-initiated payments

Card-not-present transactions typically present a higher risk of fraud.

## 13.2 Fraud Risk by Payment Channel

Different payment channels carry different risk levels:

- Face-to-face payments with customer verification generally carry lower risk
- Online and telephone payments carry increased risk
- Transactions processed without customer interaction carry the highest risk

Understanding these differences helps you apply appropriate controls.

## 13.3 Your Responsibilities in Reducing Fraud

**You're responsible for taking reasonable steps to reduce fraud. This includes:**

- Using approved payment methods and channels
- Applying recommended security measures
- Training staff to identify suspicious behaviour
- Monitoring transaction patterns

Authorisation approval alone does not remove fraud risk.

## 13.4 Indicators of Potential Fraud

**Warning signs may include:**

- Unusually large purchase amounts
- Multiple declined attempts followed by an approval
- Requests for rapid delivery or unusual delivery addresses

- Customers unable to provide consistent details

If something appears suspicious, you should pause and carry out additional checks.

### 13.4.1 Passwords

- You're responsible for **keeping your password secure** and managing how it's used to access the portal.
- If you forget your password, you can **reset it easily** using the **"Forgot your password?"** link on the login page.
- If you've forgotten the **email address** you use to log in:
    - Ask someone in your business with **administrator access** to check it in the **Teams** section of the portal.
    - If you're the **only administrator**, contact the **customer helpdesk** via the **"Chat now"** button or call **0345 901 0001**.
- Always use a **strong, unique password**, including a mix of letters, capitals, numbers, and symbols, and avoid frequently used words.

## 13.5. Strong Customer Authentication and 3D Secure

### 13.5.1 What Is Strong Customer Authentication?

**Strong Customer Authentication (SCA)** is a regulatory requirement designed to reduce fraud. It means customers must confirm their identity using extra security checks for certain payments.

SCA requires additional verification to confirm the customer is authorised to make a payment.

### 13.5.2 How Strong Customer Authentication Works

SCA requires at least two forms of verification from different categories:

- Something the customer knows (such as a password)
- Something the customer has (such as a phone)
- Something the customer is (such as a biometric feature)

This additional step reduces the likelihood of unauthorised payments.

### 13.5.3 What Is 3D Secure?

**3D Secure** is a security process used for card-not-present transactions to support Strong Customer Authentication.

**When 3D Secure is applied:**

- The transaction may be redirected for additional verification
- The customer completes authentication with their card issuer
- The issuer confirms the result

### 13.5.4 Impact on Liability

**In many cases:**

- Successful 3D Secure authentication can shift fraud liability away from the merchant
- Transactions without required SCA may be declined or disputed

You should ensure that your online and remote payment channels support 3D Secure where applicable.

# 14. Data Security and PCI DSS Compliance

## 14.1 Protecting Payment Data

When you accept card payments, you handle sensitive information. Protecting this information is essential to:

- Maintain customer trust
- Prevent fraud
- Comply with legal and contractual obligations

Make sure you ensure that payment data is protected at all times.

## 14.2 What Is PCI DSS?

**The Payment Card Industry Data Security Standard (PCI DSS)** is a global set of security standards. It explains how businesses must handle card data safely when they store, process, or transmit it.

All merchants accepting card payments must comply with PCI DSS requirements, regardless of size.

## 14.3 Your PCI DSS Responsibilities

**Your responsibilities may include:**

- Completing annual PCI compliance validation
- Using approved payment solutions

- Never storing sensitive card authentication data
- Ensuring systems are kept secure

If additional requirements apply to your business, you will be informed and supported.

### 14.4 Consequences of Non-Compliance

**Failure to comply with PCI DSS may result in:**

- Financial penalties
- Increased transaction fees
- Increased fraud exposure
- Suspension or termination of payment services

Maintaining compliance helps protect both your business and your customers.

## 15. Record Keeping and Transaction Retention

### 15.1 Why Record Keeping Is Important

**Keeping accurate and secure records is a critical part of accepting payments. Records support:**

- Customer queries and complaints
- Refund processing
- Chargeback and dispute responses
- Financial reconciliation and accounting
- Regulatory and contractual compliance

Poor or missing records are a common reason why merchants lose disputes, even when a transaction was legitimate.

### 15.2 Types of Records You Must Keep

**You should retain records relating to:**

- Completed payment transactions
- Authorisations and approvals
- Refunds and reversals
- Chargebacks and dispute correspondence

- Proof of delivery or service provision
- Customer consent for recurring or ongoing payments

**Records may exist in physical or electronic form, but they must be:**

- Accurate
- Readable
- Secure
- Accessible when required

## 15.3 Retention Periods

**Transaction records should be retained for a sufficient period to:**

- Meet card scheme requirements
- Support dispute resolution
- Meet legal and tax obligations

In many cases, records may need to be kept for several years. You're responsible for ensuring retention periods are appropriate for your business.

## 15.4 Secure Storage of Records

**All records must be stored securely to prevent:**

- Unauthorised access
- Loss or damage
- Accidental disclosure

Access to sensitive information should be limited to authorised staff only. Records containing personal data must be handled in line with data protection laws.

# 16. Staff Access, Training, and Internal Controls

## 16.1 Managing Staff Access

**Only staff who need access to payment systems should be granted it. This includes:**

- Card machines
- Online portals
- Virtual terminals
- Reporting tools

**Access should be:**

- Role-based
- Reviewed regularly
- Removed promptly when no longer required

Shared logins must not be used.

## 16.2 Staff Training Requirements

**Staff involved in payment processing must be trained so they understand:**

- How to process payments correctly
- How to handle refunds and reversals
- How to identify suspicious behaviour
- How to protect customer data

**Training should be refreshed:**

- When procedures change
- When new payment methods are introduced
- At regular intervals

## 16.3 Internal Controls

Internal controls help ensure consistent processing and reduce risk. Controls may include:

- Separation of duties
- Transaction approval thresholds

- Monitoring activity logs
- Regular reviews of reports

Mistakes or misuse by staff are treated as merchant issues and remain your responsibility.

# 17. Prohibited and Restricted Activities

## 17.1 Understanding Prohibited Transactions

Certain goods, services, or transaction types are not permitted under:

Based on industry standards These items are banned from sale, import, or payment processing.

- Illegal Narcotics and Drugs: Including illegal substances and tools intended for their production.
- Weapons and Explosives: Firearms, ammunitions, military weapons, and explosive devices.
- Counterfeit Goods: Trademarked goods, counterfeit money, and illegally copied materials.
- Pornographic Materials: Obscene or sexually explicit content.
- Dangerous Chemical Substances: Hydrofluoric acid, cyanide-related products, and prohibited ozone-depleting substances.
- Illegal Wildlife/Endangered Species: Products made from endangered animals.
- Illegal Gambling/Activities: Unlicensed casinos, money laundering services, and child exploitation materials.

## 17.2 Examples of Prohibited Activities

**Examples of prohibited or restricted activities may include:**

- Illegal goods or services
- Misrepresentation of goods or services
- Transactions designed to bypass controls
- Processing payments on behalf of third parties without approval

This list is not exhaustive.

## 17.3 Your Responsibility to Comply

**You're responsible for ensuring that:**

- Your business activities are permitted
- Your payment acceptance matches your approved business model
- Changes to your business are communicated

Failure to comply may result in suspension or termination of services.

# 18. Account Changes, Updates, and Notifications

## 18.1 Why You Must Notify Changes

Your payment services are set up based on information you provided during onboarding. You must notify Tyl by NatWest if this information changes.

**Examples include changes to:**

- Business ownership
- Business activities
- Trading names
- Bank account details
- Contact information

## 18.2 How Changes May Impact Your Account

**Some changes may require:**

- Additional checks
- Updated documentation
- Changes to approved payment channels

**Failing to notify changes may:**

- Delay settlements
- Result in declined transactions
- Breach your agreement

## 18.3 Keeping Contact Details Accurate

Accurate contact details ensure that:

- Important notifications are received
- Chargeback requests are not missed
- Support can be provided when required

You're responsible for keeping contact details up to date.

Please visit Making changes to my Tyl account on the Tyl website for more information.

# 19. Service Issues, Declines, and Troubleshooting

## 19.1 Understanding Transaction Declines

**A transaction may be declined for many reasons, including:**

- Insufficient funds
- Incorrect card details
- Fraud checks by the card issuer
- Regulatory requirements

Declines do not necessarily indicate a fault with your systems.

## 19.2 What to Do When a Transaction Is Declined

**If a transaction is declined:**

- Do not attempt to force or bypass the decline
- Advise the customer to contact their card issuer
- Avoid retrying the transaction repeatedly

Repeated attempts may increase fraud risk.

## 19.3 Service Interruptions

**Occasionally, service interruptions may occur due to:**

- Technical issues
- Network outages
- Planned maintenance

**You should:**

- Follow guidance provided during outages
- Avoid unauthorised offline processing
- Resume normal processing once services are restored

## 19.4 Getting Support

**If issues persist:**

- Use the official Tyl by NatWest support channels
- Provide clear details of the issue

- Retain any reference numbers provided

Timely support helps minimise disruption to your business.

# 20. Fees, Invoicing, and Statements

## 20.1 Understanding Fees

When you accept payments through Tyl by NatWest, fees apply for the services provided. These fees may include:

- Transaction processing fees
- Monthly service or equipment fees
- Chargeback fees
- Optional service fees

Full details of applicable fees are set out in your **Merchant Services Agreement** and related pricing schedules.

## 20.2 Invoices

Invoices summarise the fees charged to your account over a set period. Invoices typically include:

- A breakdown of fees by type
- The period covered
- The total amount due

Invoices are normally made available through your customer portal. You should review invoices carefully to ensure they align with your expectations and transaction activity.

### 20.2.1 Reviewing invoices

**Regularly reviewing your invoices helps you:**

- Understand your payment activity
- Identify unusual charges
- Detect potential issues early

If you believe an invoice contains an error, you should contact support promptly with relevant details.

## 20.3 Direct Debits and Fee Collection

**Fees may be collected:**

- Separately from settlement funds, or
- Deducted directly from settlement amounts

The method depends on your agreed settlement arrangement.

**You should ensure that:**

- Your bank account has sufficient funds
- Direct Debit details remain accurate

Failure to settle fees may result in account restrictions.

# 21. Complaints and Escalation

## 21.1 Raising a Complaint

If you're dissatisfied with any aspect of the service provided by Tyl by NatWest, you may raise a complaint.

**Complaints may relate to:**

- Service performance
- Support interactions
- Billing or settlements

**You should provide:**

- A clear description of the issue
- Relevant dates and references
- Any supporting documentation

## 21.2 Complaint Handling Process

**Once a complaint is raised:**

- It will be reviewed by the appropriate team
- You may be contacted for additional information
- We'll respond within the applicable timeframes.

Tyl by NatWest aims to resolve complaints fairly and promptly.

## 21.3 Escalating a Complaint

If you're not satisfied with the outcome of a complaint:

- You may request escalation
- Further review will be conducted

Details of escalation options are available under 'How do I make a complaint' on the Tyl website.

# 22. Suspension and Termination of Services

## 22.1 When Services May Be Suspended

Tyl by NatWest may suspend payment services where necessary, including cases of:

- Suspected fraud
- Excessive chargebacks
- Breach of agreement
- Regulatory or legal requirements

Suspension may be temporary or ongoing, depending on the issue.

## 22.2 Termination of Services

In more serious cases, services may be terminated. Termination may occur where:

- Issues are not resolved
- Risk remains unacceptable
- Contractual obligations are not met

Termination is carried out in line with your Merchant Services Agreement.

## 22.3 Your Responsibilities Following Termination

If services are terminated, you remain responsible for:

- Outstanding fees
- Ongoing disputes or chargebacks
- Record retention obligations

Termination does not remove liability for past transactions.

# 23 Legal and Regulatory Framework

## 23.1 Applicable Laws and Regulations

Payment services operate within a legal and regulatory framework. This includes:

- Payment services regulations
- Consumer protection laws
- Data protection legislation
- Card scheme rules

You're responsible for ensuring your business complies with all applicable requirements.

## 23.2 Data Protection Obligations

When handling customer data, you must:

- Process data lawfully
- Use data only for legitimate purposes
- Protect data against unauthorised access

These obligations apply in addition to PCI DSS requirements for card data.

## 23.3 Regulatory Changes

Regulatory requirements may change. You should:

- Stay informed of updates
- Adjust your processes where necessary
- Follow updated guidance provided by Tyl by NatWest

# 24. Glossary of Terms

This glossary explains key terms used throughout the manual.

**Authorisation**
The process of confirming with a card issuer that a transaction may proceed.

**Card Issuer**
The bank or financial institution that issued the payment card to the customer.

**Card-Not-Present Transaction**
A transaction where the customer and card are not physically present.

**Card-Present Transaction**
A transaction where the customer and card are physically present and the card is processed using a card machine.

**Chargeback**
A disputed transaction returned to the customer's card following a claim raised with their card issuer.

**Contactless Payment**
A payment completed by tapping a card or device against a card machine.

**Digital Wallet**
A service that securely stores card details on a device for payments.

**Merchant**
A business that accepts electronic payments for goods or services.

**Settlement**
The transfer of funds from completed transactions into the merchant's bank account.

**Strong Customer Authentication**
Additional verification required for certain electronic payments to reduce fraud.

# 25. Frequently Asked Questions (FAQs)

This section answers common questions merchants ask when using Tyl by NatWest services. It is intended as a quick reference alongside the main sections of this manual.

## 25.1 Account Access and User Management

**Can I create users for my team with different levels of access?**

Yes. You can add and manage users with different access levels through the customer portal.
This allows you to control who can:

- View transactions and payouts
- Process refunds
- Access reporting
- Manage settings

User access should be limited to staff who need it to perform their role.

**What should I do if I cannot log in or receive an "invalid email" message?**

You must use the email address registered to your Tyl by NatWest account. If:

- The email address is incorrect, or
- The email does not belong to the account owner

You may receive an error during login or verification.

If you're unsure which email address is registered, an administrator user in your business can check this in the portal. If you're the only administrator, contact merchant support for assistance.

**What does an "in progress" status mean in the mobile app?**

An "in progress" status means your account is still being set up or verified.
You will receive confirmation when setup is complete.

If the status remains unchanged for an extended period, contact merchant support.

## 25.2 Transactions and Reporting

**How can I view my transactions?**

You can view transactions through the customer portal.
Transactions can be filtered by:

- Date range
- Status
- Payment method

This allows you to review activity, identify issues, and reconcile settlements.

**Why can't I export all of my transactions?**

Transaction exports may be limited to a maximum number of rows per file.
If your export exceeds this limit, you may need to:

- Reduce the date range
- Apply additional filters
- Run multiple exports

**What do different transaction statuses mean?**

Common transaction statuses include:

- **Successful** – The transaction was approved
- **Declined** – The transaction was rejected by the card issuer
- **Cancelled or voided** – The transaction was stopped before settlement
- **Refunded** – The original transaction has been refunded
- **Partially refunded** – Only part of the transaction amount was returned

## 25.3 Payment Links

**What is the minimum amount for a payment link?**

Payment links can be created for very small amounts, starting from the minimum supported value in your currency.

**What is the maximum amount for a payment link?**

Payment links have a maximum value and is subject to scheme, regulatory and issuer changes. If you need to send links for a higher amount, you can contact customer service team on **0345 901 0001** who can update this for you.

This limit may be adjusted in certain circumstances by contacting merchant support.

**How long is a payment link valid for?**

When creating a payment link, you can choose an expiry date between 5 and 60 days. Expired payment links cannot be used and must be re-issued if payment is still required.

**Can a payment link be used more than once?**

No. Once a payment link has been successfully paid, it expires automatically and cannot be reused.

**Can customers make partial payments using a payment link?**

Partial payments are not supported.
Once a payment link has been used successfully, it is completed and closed.

**What happens if a payment link is not paid?**

If a payment link is not paid before it expires:

- No funds are taken
- The link automatically becomes inactive

You may generate a new link if required.

**Where can I view payment links I have sent?**

You can view payment links and their status:

- In the customer portal
- In supported mobile applications

This includes whether the link is active, paid, or expired.

## 25.4 Refunds

**How do I issue a refund?**

Refunds must always be issued to the original payment method used by the customer.
The process depends on how the original transaction was taken:

- Online payments are refunded through the Virtual Terminal or API (Virtual Terminal user guide)
- Card-present payments are refunded using the card machine (please refer to guides found in the Tyl help and Support section)

Follow the refund procedures outlined earlier in this manual.

**How long do refunds take to reach the customer?**

Most refunds are processed promptly once submitted.

However, the time it takes for funds to reach the customer depends on their card issuer and bank.

Delays may occur:

- Over weekends or bank holidays
- Where additional checks are required

**What should I do if a refund fails or is declined?**

If a refund request is declined:

- Check that the original transaction exists
- Confirm sufficient funds are available
- Ensure the correct refund process was followed

If the issue continues, contact merchant support.

## 25.5 Payit (Open Banking Payments)

**How do refunds work for Payit payments?**

Refunds for Payit payments are handled differently from card payments.
Refunds are processed back to the customer's bank account rather than a card.

Processing time depends on:

- When the refund is submitted
- Bank processing schedules

**Does Payit payments use a chargeback process like card payments?**

- Payit transactions **do not typically include Section 75 protection or card chargeback rights**.
- However, you're **still legally protected**:
    - The **Consumer Rights Act 2015** covers you if goods are faulty or not as described.
    - The **Payment Services Regulations** protect you against **unauthorised payments**, no matter how you paid.

**Disputes and problems with purchases**

- Payit works through **bank-to-bank payments**, and there is **no chargeback scheme** like those used for card payments.
- If you have an issue with a purchase, you should:
    - Contact the **retailer** first, or
    - Speak directly with **your bank** for further support.

**How long does it take for a refund to be processed on Payit?**

- We will process the majority of refund transactions on the same day or the following day.
    - Example: a refund request for a payment transaction, where the payment transaction was made several weeks ago.

Payments are sent 7 days a week at around 23:00-23:59.

However, in some cases, the payments take longer. This is usually the result of either:

1. Your customer has submitted the payment and/or refund requests during a non-working period (i.e. a weekend or bank holiday)

2. Waiting for account details – a bank file that needs to match the initial payment transaction. We can't process a refund transaction until we check this match. The rule to look at is: We'll match the account details to the payment transaction. After that, the refund process can begin.

## 25.6 Support and Troubleshooting

**Who should I contact if I need help?**

If you need assistance with:

- Transactions
- Refunds
- Chargebacks
- Account access
- Technical issues

You should contact Tyl by NatWest merchant support using by visiting our help and support page, or by calling us on **0345 901 0001**

**Note:** To contact us using Text Relay, add **18001** before any of our phone numbers.

**What information should I provide when contacting support?**

Providing the following information will help resolve issues more quickly:

- Your merchant details
- Transaction references
- Dates and amounts
- A clear description of the issue