

EMIL.

Strong Customer Authentication

Cardholder Journey



What is Strong Customer Authentication (SCA)?

SCA is a European requirement introduced to make online interactions more secure and reduce the risk of fraud. These requirements were part of the Revised Payment Services Directive (PSD2). PSD2 requires banks to implement multi-factor authentication to qualifying remote transactions like online payments and access to payment account.

This requirement applies to the European Economic Area (EEA), Monaco, and UK.

SCA means users may need to complete extra levels of authentication for remote transactions like online payments and access to payment account. These levels of authentication involve asking customers for two of the three following:

- **something they know (Knowledge factor)**
- **something they own (Possession factor)**
- **something they are (Inherence factor)**

Before SCA, issuing banks could only challenge customers with a single static password. These new dynamic data points verify users' identities more accurately.



EML's SCA Solution

Our solution supports two factor authentication using the following:

- **Memory Word:**
 - Cardholder will be required to set up memory word which can then be used as a knowledge factor for authentication.
 - Memory word is case sensitive, has maximum length of 45 characters (including spaces) and accepts standard UTF-8 characters.
- **One Time Password (OTP):**
 - Cardholder's registered mobile number will be used to send a one-time password (OTP).
 - If no mobile is available OTP will be sent to the registered email.
 - **All CCP users must have a registered mobile number or email with PFSL or they will not be able to access CCP.**



Impacted Journeys

All CCP users must have a registered mobile number or email with PFSL or they will not be able to access CCP.

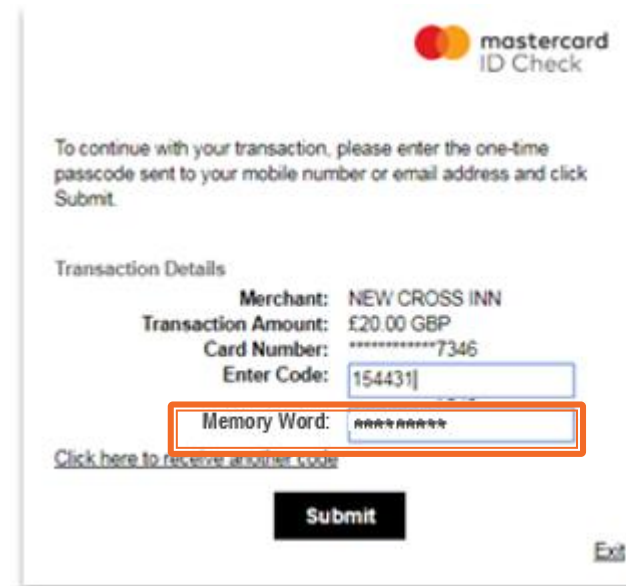
- All existing users will be required to authenticate using OTP on **first login** (post SCA implementation).
- **Every 90 days** after the last successful login, all cardholders will be required to authenticate using OTP.
- All new users will be required to **set up 'Memory word'** during the **registration journey**.
- 'Memory word' can be updated from Edit Account Details page.
- All users will be prompted to provide authentication via OTP and login password on requesting **transaction report older than 90 days**.
- All users will be prompted to provide authentication via OTP and Memory word when a **new payee is created**.
- Cardholders will be prompted to provide authentication via OTP and KBA (knowledge-based answer) on selected e-commerce transactions



E-commerce transactions (3DS authentication)

Cardholders that have set up 'Memory word' will be prompted to provide additional authentication via Memory word on eligible e-commerce transactions.

Note: If the cardholders have not yet set up Memory word, only OTP will be used to authenticate.



mastercard
ID Check

To continue with your transaction, please enter the one-time passcode sent to your mobile number or email address and click Submit.

Transaction Details

Merchant: NEW CROSS INN
Transaction Amount: £20.00 GBP
Card Number: *****7346
Enter Code: 154431
Memory Word: *****

[Click here to receive another code](#)

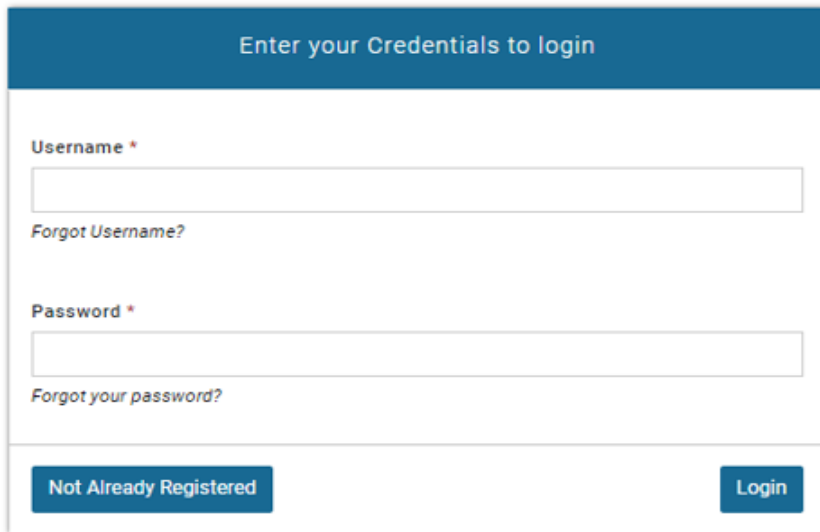
Submit

Exit

Login Journey

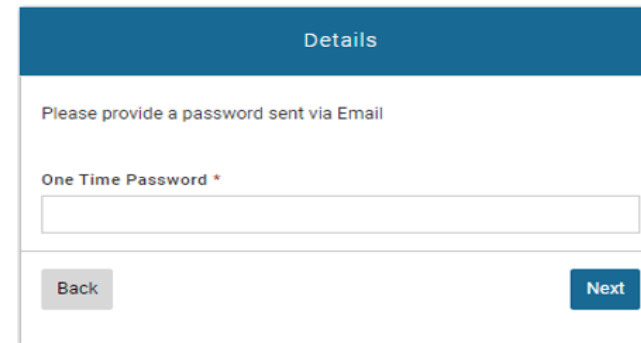
- User will be prompted to enter OTP on first login and every 90 days thereafter.
- User should have a registered mobile number or email with PFSL to receive OTP.
- If both email and mobile number are provided OTP will be sent to mobile.
- If mobile is not provided OTP will be sent via email.
- If neither mobile or email is provided login will fail with the stating, we couldn't initiate OTP.

Step 1: User enters login credentials (existing page)



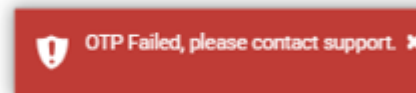
User has provided mobile or email →

Step 2: User prompted to enter OTP (new page)



User has NOT provided mobile or email →

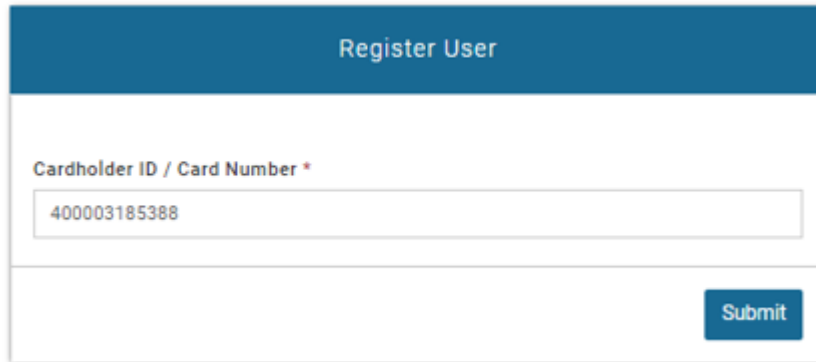
Step 2: Login Failed



Registration journey

All new users will be required to set up 'Memory word' during the registration journey.

Step 1: User enters card details(existing pages)

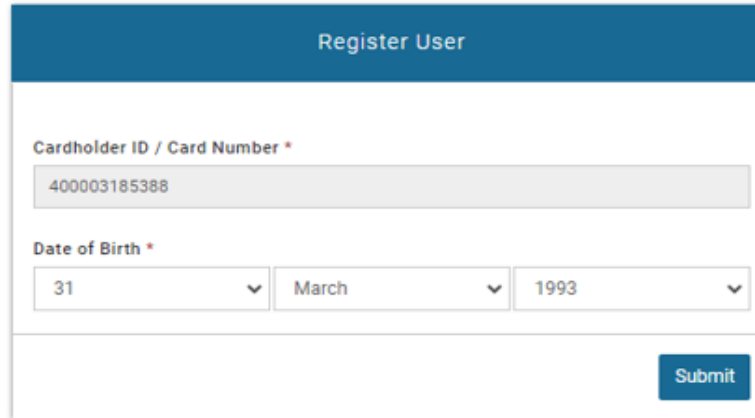


Register User

Cardholder ID / Card Number *

400003185388

Submit



Register User

Cardholder ID / Card Number *

400003185388

Date of Birth *

31 March 1993

Submit



Registration journey cont'd

Step 2: User enters details for registration (existing page with new field for Memory word)
Memory word field accepts standard UTF-8 characters, max length 45 characters

The screenshot shows a 'Register User' form with the following fields:

- Username *: Test123901
- Confirm Username *: Test123901
- Password *: [masked]
- Confirm Password *: [masked]
- Security Question *: Mother's maiden name
- Security Answer *: Test
- Memory Word *: [masked]
- Confirm Memory Word *: [masked]

A red box highlights the Memory Word and Confirm Memory Word fields. Below the Memory Word field, there is a note: "Please provide a memorable word. You will be required to provide this word when you wish to add a new payee." A blue 'Submit' button is located at the bottom right of the form.

Step 3: User registered successfully. (existing page)

The screenshot shows the 'Register User' page after successful registration. The message "Details were successfully registered." is displayed in the center. Below the message is a link labeled "Return to Login".

Edit Memory Word

'Memory word' can be updated from Edit Account Details page.

EDIT ACCOUNT DETAILS

Email *	<input type="text" value="Please enter Email Address"/>
Confirm Email *	<input type="text" value="Please Confirm Email Address"/>
Memory Word	<input type="password" value="*****"/>
Confirm Memory Word	<input type="password" value="*****"/>

[Update Details](#)



Transaction History

All users will be prompted to provide authentication via OTP and login password on requesting transaction report older than 90 days.

Step 1: On Transaction History page, user selects a date range older than 90 days.

Step 2: User is prompted to enter OTP and login password. Note: There is no limit on incorrect attempts.

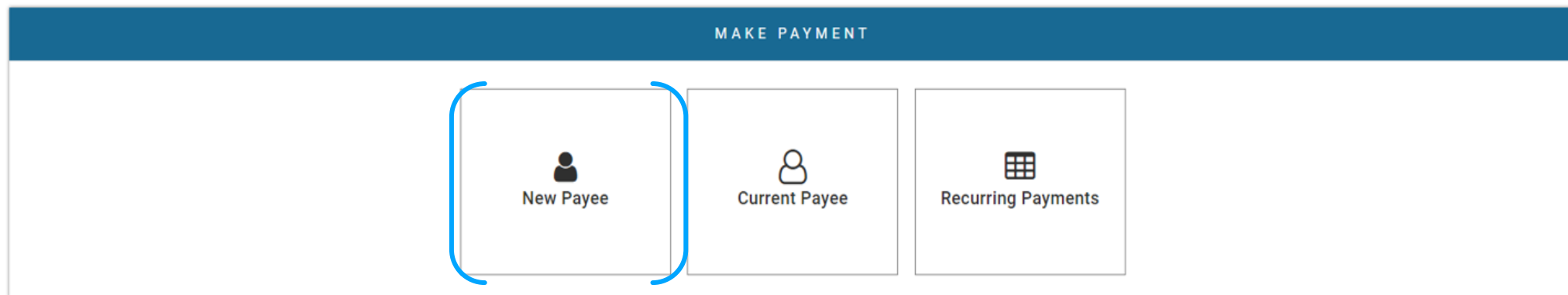
The screenshot displays the 'TRANSACTION HISTORY' interface. At the top, a blue header contains the text 'TRANSACTION HISTORY'. Below this, a light blue bar shows 'Ledger Balance'. A red warning icon and text state: 'There are no transactions associated with the selected date range'. Below the warning, the text 'Select a date range to view your transactions' is followed by two rows of date selection: 'Date from' (26 June 2023) and 'Date to' (3 July 2024). A 'Get Transactions' button is located at the bottom right of the date selection area. A modal window titled 'Confirm Authentication' is overlaid on the page. It contains the text 'Please provide a password sent via Email' and two input fields: 'One Time Password *' and 'Password *'. At the bottom of the modal are 'Cancel' and 'Confirm' buttons.

Add a Payee

All users will be prompted to enter 'Memory word' and OTP when a new payee is added.

Note: There is no limit on incorrect attempts..

Step 1: On Make Payment page user selects New Payee (existing page)



Add a Payee cont'd

Step 2: User enters payee details (existing page)

MAKE PAYMENT

Please fill in form to continue, if you wish to select current payee [click here](#).

Creditor Sort Code*

Creditor Account Number*

First Name*

Last Name*

[Start Over?](#)

Step 3: User is prompted to enter OTP and Memory word. (new page) Note: There is no limit on incorrect attempts.

MAKE PAYMENT

One Time Password was sent to you via Email

One Time Password*

Memory Word*

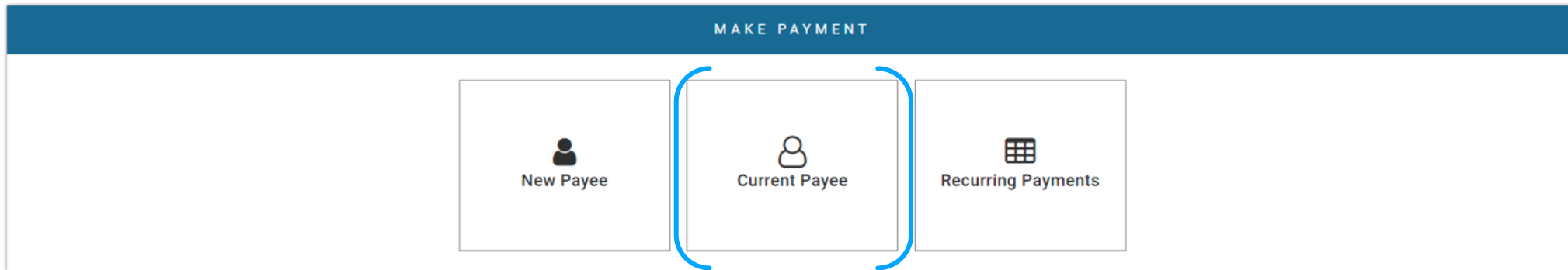
[Start Over?](#)

Create a new recurring payment

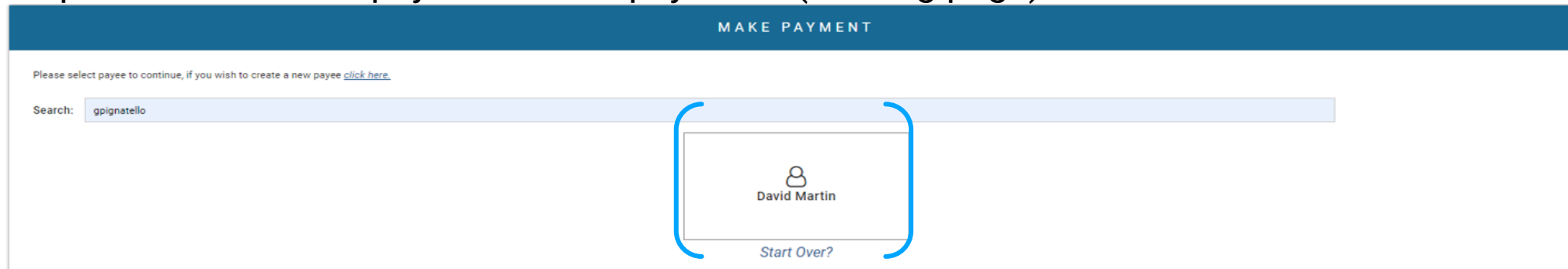
All users will be prompted to enter 'Memory word' and OTP when a new recurring payment plan is created.

Note: There is no limit on incorrect attempts.

Step 1: On Make Payment page user selects Current Payee.(existing page)



Step 2: User selects a payee from the payee list.(existing page)



Create a new recurring payment cont'd

Step 3: User selects 'Make a set number of payments and the stop'. (existing page)

MAKE PAYMENT

Make a one off payment

Make a set number of payments and then stop

Make payments until a specified date

Start Over?

Step 4: User enters the details for recurring payment and clicks Submit. (existing page)

MAKE PAYMENT

Available Balance: GBP 10.00

Payee selected: David Martin ✓

Please fill in the fields to Continue, if you wish to change payment type [click here](#).

Payment Type* Care Agency

First payment date * 12 July 2024

First payment amount* 10.00

Payment Reference* assaddsaasd

Further payment(s) amount* 10.00

Frequency* Weekly

Total Number Of Further Payments* 4

Invoice No/Ref No

Extra Details

Submit

Start Over?



Create a new recurring payment cont'd

Step 3: User is prompted to enter OTP and Memory word (new page). Note: There is no limit on incorrect attempts.

MAKE PAYMENT

Review

Payee Name	David Martin
Payment Method	Recurring payment
Payment Type	Care Agency
Reference	asdsasadd
First Payment Date	2024/07/12
First Payment Amount	GBP 10.00
Further payment(s) amount	GBP 10.00
Frequency	Weekly
Total Number Of Further Payments	4

Submit

OTP Required

One Time Password *

Memory Word *

Start Over?

Thank you

