NL PSD2 SCA – Frequently Asked Questions

Programme Administrators

GENERAL

1. Why are online purchases, contactless and Account access journey changing?

From 14 September 2019, a key part of the EU Revised Payment Service Directive (PSD2) is coming into effect. A key element of PSD2 is the introduction of additional security authentications for online transactions, known as Strong Customer Authentication (SCA). Its focus on security means all card issuers will need to verify a cardmember's identity more often when making purchases online, in-store with contactless and when logging into his/her online Account.

For online card payments, these requirements will apply to all American Express Cards issued in EU countries and the European Economic Area (EEA) and applies when used with an EEA merchant.

The EU countries are:
Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

The European Economic Area (EEA):
The EEA includes EU countries plus Iceland, Liechtenstein and Norway.

2. Who does PSD2 affect?

PSD2 impacts anyone involved in the buying and selling of goods and services in the EU. Consumers, financial institutions, and the payments industry including aggregators and account information service providers are all affected by PSD2.

3. What is two factor authentication/SCA?

PSD2 requires the use of two independent sources of validation by selecting a combination of two out of the three categories (commonly known as the 'two-factor authentication'):

- something you know (e.g. PIN)
- something you have (e.g. card/phone)
- something you are (e.g. fingerprint)

SCA will apply to "customer-initiated" online payments within EEA.

4. How will Account login change?

Cardmembers will receive a verification request when they access their Account online. When they log into their online American Express Account, they will need their username and password as usual. American Express may send them an extra verification request by text or email when they are trying to access certain parts of their Account such as viewing their PIN.

In addition, Business Card, Corporate Card, Corporate Meeting Card, Corporate Purchasing Card Cardmembers accessing their Online Account and users of vPayment and Buyer Initiated Payments portals will see more verification requests as well.

5. Is there any inactivity period to be taken into consideration when accessing Online Accounts?

The regulation specifies *'...a maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes...'*

This applies to all impacted online portals (such as vPayment, Buyer Initiated Payments and FXIP portals), including a Cardmember's American Express Online Account. When exceeding the five minutes of inactivity, a new verification request will be sent to the Cardmember and/or Account user.

6. What products are impacted by these changes?

At this point, all American Express Cards, including Corporate Cards and Corporate Meeting Cards, issued in the European Economic Area (EEA) are impacted by the changes to online transactions.

We will keep you informed of any further updates.

7. How will online payments change?

Cardmembers will see SafeKey® more often.

From 14 September 2019, Cardmembers will see SafeKey appear during the checkout stage more often. SafeKey helps protect against fraud while shopping online by confirming it's really the Cardmember making the purchase. Cardmembers will also receive verification requests by text or email more often, as they complete their online payments.

8. How will contactless payments change?

Cardmembers will be asked more often to enter the PIN code for contactless payments. Most of the time they will be able to use their contactless Card as usual. However, they may be asked more often to enter the PIN code. The terminal will ask the Cardmember to place his/her Card in the card reader and enter the PIN code.

If they have forgotten their Card PIN, they can see it in their online Account.

9. Corporate Exemptions to Strong Customer Authentication (SCA)

American Express acknowledges the industry wide challenges and is working towards minimising the friction for corporate travel payments. We are actively addressing and developing solutions to ensure compliance with the PSD2 Strong Customer Authentication (SCA) requirements. We believe that our lodged* or virtual corporate products satisfy the corporate exemption criteria. We are taking full advantage of the corporate exemption as specified by the European Banking Authority's Strong Customer Authentication standards.

** A lodged Card is for example used to pay for corporate travel with the Business Travel Account (BTA) via a Travel Management Company.*

10. Exemptions

Not all transactions will require additional authentication; certain types of transactions are either "Out of Scope" or "Exempt". This includes purchases by email or telephone (Mail Order/Telephone Order) or transactions via trusted beneficiaries (Express List – see question 19).

American Express is responsible for ensuring the appropriate treatment is applied and this should be transparent to the Cardmember.

11. Does SCA apply to recurring billing?

SCA is only required on initial transaction initiated by the Cardmember.

Subsequent transactions initiated by the Merchant (Merchant Initiated Transactions) are exempted. These transactions are initiated without any interaction or involvement of the Cardmember.

There is no impact to existing set ups.

A recurring payment (billing) is a Card on File (COF) transaction. A series of recurring payments consists of multiple transactions that are billed to a Cardmember at fixed, regular intervals not to exceed one year between transactions.

The series of recurring payments is the result of an agreement between the Merchant and the Cardmember, where the Cardmember has given a mandate authorising the Merchant to provide products or service. You can think of software licenses, online advertising costs, mobile phone bills or other subscriptions.

The initial transaction in a series usually requires SCA. The subsequent transactions are qualified as Merchant Initiated Transactions and are generally exempt. When the Cardmember amends the series/arrangements, SCA must be applied accordingly.

12. How does SCA work when a Card is lodged with a TMC (Travel Management Company) or with a Travel Booking tool?

The Financial Conduct Authority has acknowledged in its PSD2 guidance document that lodged or virtual corporate Cards, such as those used within an access-controlled corporate travel management or corporate purchasing system, would be within scope of the corporate exemption, provided certain criteria are met. We expect other regulators will take a similar view. At the moment, De Nederlandsche Bank and Banco de España have not yet made a statement about this. As such, American Express intends to rely upon the corporate exemption for transactions initiated using these products and is working with regulators across the EEA to validate this position. Our primary consideration is to ensure that service to our merchants and Cardmembers continues as normal. Any change on this position will be shared with our corporate clients.

13. At what limit is SCA triggered online, when should a Cardmember expect to see it?

SCA applies to all transactions regardless of the amount, exemptions may apply. Card transactions below €30 are considered low value and are generally exempt from authentication.

14. Why do Account users and Cardmembers need to update their contact details?

From 14 September 2019, two factor authentication is required for all Account users, Corporate Card and Corporate Meeting Card Cardmembers who transact online. The regulation is specific to the individual to whom the card is registered with and is making the purchase. If requirements are not met, the issuer must decline the transactions. It is therefore important that we have up-to-date email addresses and mobile numbers of Cardmembers to be able to send a one-time verification code to the Cardmembers.

15. How can Cardmembers and Account users update their contact details?

Cardmembers can update their contact details (email address and mobile number) in their online profile with Concur and/or travel agency and in their American Express Online Account. Alternatively, they can contact the American Express Customer Service team using the number on the back of their Card.

vPayment users can update their contact details by asking their Admin or by contacting the Servicing team. An Admin can go in the vPayment OnDemand portal, in the section "Administration/Manage users" and edit the user profile. A user can call the Servicing team directly to change his/her password or contact details.

BIP users can amend their own contact details in the BIP portal itself once they are logged in.

16. How will contact details be used and stored?

American Express takes privacy seriously and we will not use contact details for marketing purposes without Cardmembers' and Account users' consent. Contact details will be stored in accordance with our privacy policy which can be accessed via americanexpress.nl/privacy-statement

17. If someone else does the booking on behalf of a Cardmember, can the Cardmember share his/her data?

When booking online, the Cardmember is the only person who may use the Card and is responsible for the authorisation of a transaction if the Card is in the Cardmembers' name. The verification code is sent to the registered contact details of the Cardmember.

If someone else makes a booking through a corporate travel management system or corporate purchasing system on behalf of the Cardmember, the scenario of question 8 may apply.

18. What is a (one-time) verification code?

It is a (one-time) 6-digit code sent via SMS and/or email that Cardmembers need to enter into the SafeKey screen or Online Access login screen to verify it's them. This layer of security lets us know it is the Cardmember him/herself who makes the purchase, because we are sending the code to their registered contact details.

19. What is Express List?

Express List is a service we provide to American Express Cardmembers only, enabling cardmembers to populate a list of merchants they trust and frequently shop with. When they add certain webshops (merchants) to their trusted Express List, they will be sent fewer verification codes when making purchases and complete transaction faster, while still getting the same protection that American Express always offers.

My Express List is a standard feature of the SafeKey journey.

20. How do Cardmembers set up Express List?

Cardmembers can set up Express List as part of a SafeKey journey. It will allow them to select individual merchants or 'select all' merchants where they regularly make online purchases (up to 100 merchants).

21. Will Cardmembers be able to manage their list of merchants in their Express List?

Cardmembers who have an American Express online account can (soon) manage the Express List themselves. As soon as this functionality is available for the Netherlands, we will inform the Cardmembers accordingly.

This functionality is already/will be available for the following countries: Austria, Belgium, France, Germany, Italy, Norway, Spain, Sweden, The Netherlands & UK.

22. How do Cardmembers register for an American Express Online Account?

Cardmembers can create an online account via americanexpress.nl/registreren (Dutch only)

23. Do Cardmembers need to register for American Express SafeKey?

Cardmembers are automatically enrolled for American Express SafeKey. There is no additional step that the Cardmember needs to take for existing or new Cards other than ensuring the mobile phone number and/or email address on file with American Express is updated for his/her American Express Card(s).

24. A Cardmembers' transaction has failed. What does he/she need to do?

Different reasons could cause the failure of a transaction, for example when the one-time verification code was entered incorrectly or some of the security questions have not been answered correctly. In that case, access to SafeKey could be blocked. If the verification code wasn't entered correctly after three attempts, the transaction will expire. Technical issues in the payment service of the merchant could also interrupt the transaction. If the transaction is unsuccessful the Cardmember will receive an on-screen notification. If the Cardmember needs any assistance, he/she can call Customer Services via the number on the back of the Card.

25. How quickly will Cardmembers get a verification code?

Cardmembers will immediately receive a verification code to the email address and/or mobile phone number that American Express has on record (if we have those records). A verification code is only valid for ten minutes from the time Cardmembers submit their Card details to the merchant. If a Cardmember does not complete their transaction during the ten minutes, the transaction will need to be restarted.

26. Will SCA impact the way Cardmembers pay their bills?

No, there is no change to the way bills are paid.

27. Are replacement Cards impacted?

SCA will apply to all American Express Cards issued in the EEA.