

Frequently Asked Questions

Learn more about the TransactVerify app

- A) The app in general
- B) About Mastercard® Identity Check™ (3D Secure)
- C) Payment with Mastercard® Identity Check™ (3D Secure)
- D) About eStatement (card billing)
- E) Information on how to view transactions
- F) Information about the Alert Service
- G) Administration
- H) Security and privacy

A) The app in general

1. What are the technical requirements for your mobile device for using the "TransactVerify" app?

"TransactVerify" is made available for the current version of the smartphone operating systems Android (from 9.0) and iOS (from 15). The app is offered free of charge in the App Store and Google Play Store.

Newer smartphone models with the Android and iOS operating systems support the "Fingerprint/Touch ID or Face ID" function. This function must be activated in the settings of your smartphone and the feature must be stored accordingly so that it can be used for authentication using Mastercard® Identity Check™ (3D Secure) for payments on the Internet.

2. What devices can I use?

Smartphones and tablets can generally be used; however the app is optimized for use on smartphones due to special features in the display (only upright).

3. What are the system requirements of Mastercard® Identity Check™ (3D Secure)?

Mastercard® Identity Check™ does not require any special software, but an up-to-date browser that supports the TLS 1.2 encryption protocol for a secure connection. All available security updates should be installed. In addition, you need to disable software that blocks the display of pop-up windows. This would lead to conflicts in the use of the procedure.

You can only approve your payment via fingerprint (Touch ID) or facial recognition (Face ID) if your smartphone supports the "Fingerprint/Touch ID" or "Face ID" function and you have stored your biometric feature in advance in the settings of your mobile device.

4. What other conditions should I be aware of for trouble-free use?

The use of the app with smartphones or tablets that are operated with manipulated or uncertified software (e.g. by jailbreaking or rooting) is not permitted.

5. Which cards can I register in the TransactVerify app?

You can register all Mastercard® cards from your card-issuing institution ("Card Issuer"). There is no limit to the number of cards. This applies accordingly to the use of Mastercard® Identity Check™. However, the prerequisite is that your card issuer uses First Data GmbH ("First Data") as a service provider or that First Data itself is the card issuer.

6. Can I use several mobile phones or smartphones?

No, each card number can only be registered once in the app and thus only on a smartphone. However, it is possible to change the smartphone. To do this, enter your card number in the app and follow the instructions in the app.

7. Do I need a PIN for the TransactVerify app? And what do I have to do if I have forgotten the PIN?

You must assign a 4 to 6-digit PIN when registering your card for the "TransactVerify" app, even if you decide to approve Internet payments using Mastercard® Identity Check™ (3D Secure) via fingerprint (Touch ID) or facial recognition (Face ID). In this case, you can use the PIN if your fingerprint or facial recognition is not technically possible (dirty sensor, etc.).

If you forget the PIN for the app, you will have to go through the registration process again. The PIN cannot be reset for security reasons.

8. How is the use of the app and the registration for Mastercard® Identity Check™ (3D Secure) related?

In order to use the app with a card, this card must be connected to the app. For this purpose, the registration for Mastercard® Identity Check™ is used.

9. Why can't I use all the features (functionalities) of the app?

The possibilities offered by the app depend on the features (functionalities) offered by the card issuer.

B) About Mastercard® Identity Check™ (3D Secure)

10. What is Mastercard® Identity Check™ (3D Secure)?

Mastercard® Identity Check™ (3D Secure) is a service provided by Mastercard® and your card issuer that provides additional protection against unauthorized or improper use of your card when making online payments and allows you to identify yourself to your card issuer as the authorized cardholder. There are currently the following two procedures for verifying your identity when making internet payments:

- Confirmation of payment via the "TransactVerify" app and
- Confirmation of payment via the mobileTAN or mTAN procedure. In this case, you will receive a mobile TAN on your mobile device, which you enter on the merchant's website. This procedure is independent of the TransactVerify app and is therefore not described in detail below. If you would like to use this procedure, please contact your card issuer.

The authentication of the cardholder for internet payments is generally mandatory for card issuers and payment service providers of merchants due to legal requirements (apart from defined exceptions).

11. How does Mastercard® Identity Check™ (3D Secure) protect me?

By authenticating yourself during an online payment process, you identify yourself to your card issuer as the legitimate cardholder. The Internet merchant receives a corresponding message if authentication is successful and the purchase process is completed. If you are unable to authenticate successfully, the Internet merchant will receive a message that authentication was not possible and the transaction cannot be completed.

12. How does Mastercard® Identity Check™ (3D Secure) work with the help of the app?

If you have registered the card you want to use to pay for an online purchase in the "TransactVerify" app, you will be redirected directly to the payment process with Mastercard® Identity Check™ (3D Secure) when shopping online. The payment information, in particular the merchant, amount, date and time, is listed there. If an identity check is required for the payment, you must authenticate yourself:

If you have registered your card for the "TransactVerify" app procedure, you will receive a push message on your mobile device (e.g. smartphone) and will be asked to approve the payment in the app. If you have suppressed the receipt of messages from this app in the operating settings of your device, open the app manually and approve the payment there.

Depending on your selection during registration, you will also be asked to enter either the PIN you chose during registration or the biometric recognition.

Which biometric identifier (Face ID or Touch ID/fingerprint) is used by the app depends on which of the two methods you have set in the settings of your mobile device. You can only approve your payment by fingerprint or Face ID if your smartphone supports this feature and you have stored your fingerprint or Face ID in advance in your smartphone's settings. If the biometric identifier (fingerprint or Face ID) is not recognized, you will be asked to enter the PIN you chose during registration instead.

There is also the option to approve payments offline via the QR code scanner in the app. To do this, the appropriate online method must be selected on the merchant's website. This is to be scanned with the app's QR code scanner. The app will then display a code that must be entered on the merchant's website along with the app's PIN. If entered correctly, the payment will be released via the app.

Once you have approved the payment via app, the merchant will be informed of the successful authentication and the purchase will be completed. In your browser window, you will automatically be redirected back to the online shop.

13. Can I register for both authentication methods (app and mobileTAN/mTAN)?

No, only one procedure can be used per card (card number). If your card issuer offers both methods, please contact your card issuer to change the procedure.

14. What are the advantages of Mastercard® Identity Check™ (3D Secure)?

Secure Internet payments: Mastercard® Identity Check (3D Secure) is a process that is intended to make online payments more secure by verifying your identity during the payment process. Authentication allows you to identify yourself as an authorized cardholder to the card issuer. 3D Secure thus serves to prevent abusive transactions by unauthorized third parties. All data is transmitted encrypted.

High flexibility: You can shop on the Internet from any mobile device worldwide, around the clock and pay securely with your card. Transaction approval takes place dynamically via their registered procedure (i.e. via TransactVerify app or mobileTAN). You don't need to remember an additional password unless you want to approve internet payments in the app using a PIN.

No software installation: Mastercard® Identity Check™ (3D Secure) does not require any software installation. All you need is the TransactVerify app on your mobile device. Registration and usage are uncomplicated for you.

15. What happens if I lose the card or if it is stolen?

Please report the loss immediately to your card issuer using the contact details provided by your card issuer. The card will be blocked and the blocking will automatically also apply to Mastercard® Identity Check™ (3D Secure).

If you applied for a replacement card due to the blocking, you will need to register the replacement card again.

16. What information is required for registration?

To register, only the card number is required in the first step.

Then, you will need to apply for an identification code that will help authenticate you during the registration process. Depending on the transmission method for the identification code offered by your card issuer and chosen by you, further data may then be requested. If you are requesting a code via SMS, this is the expiry date of the card, the last four digits of your account number through which your card transactions are billed, as well as your date of birth and mobile phone number. The mobile phone number must be identical to the one you have given your card issuer (e.g. in the card application).

17. How do I get an identification code?

To register your card in the app and authenticate yourself during the registration process, you will need an identification code. Your card issuer determines which of the following three ways to transmit the identification code to you:

- by SMS (after entering the additional data described in section 15)
- as part of a 1-cent credit to your billing account of the card
- by letter

18. Why do I have to provide additional data to receive the identification code by SMS?

If you wish to receive the identification code by SMS as part of the registration process, the last four digits of your account number, the expiry date of your card, your date of birth and your mobile phone number will be required. This information is compared with the data on file with your card issuer. This is an extra precaution to ensure that when you register, you are the cardholder.

19. Can I shop immediately after registration?

Yes. You can pay with Mastercard® Identity Check™ (3D Secure) on the Internet immediately after completing the registration.

20. What can I do if I have questions during registration?

If you have any questions or need help during the registration process, please contact the cardholder service of your card issuer, telephone: +49 (0) 69 / 7933-2555. This service is available around the clock.

C) Payment with Mastercard® Identity Check™

21. How do I use Mastercard® Identity Check™ (3D Secure) with the "TransactVerify" app when paying online?

If you pay at a merchant on the Internet and authentication is required, a site opens with the payment details (date, merchant name and payment amount). At the same time, you will also receive a push message with the same payment details via the "TransactVerify" app. Compare the payment details you see at the merchant with those in the app. If the information matches, confirm the payment by fingerprint (Touch ID) or facial recognition (Face ID) on your smartphone. You can only approve your payment by fingerprint or Face ID if your mobile device supports the Touch ID/Fingerprint or Face ID function in an appropriate way and you have your fingerprint or your Face ID saved in advance in the smartphone settings. Whether you confirm the payment via Touch ID or Face ID depends on the biometric procedure you have set in the settings of your mobile device.

Alternatively, you can enter the PIN you chose during registration.

Then the legitimization process is completed.

If the payment details do not match, cancel the process and contact the cardholder service of your card issuer on Tel. +49 (0)69 / 7933-2555.

22. Do I authenticate myself with Mastercard® Identity Check™ every time I shop online?

In principle, yes. However, the card issuer can use exceptions under certain conditions (e.g. depending on the amount). It is therefore also possible for an internet payment to be forwarded for authorization even without authentication.

23. Can I buy from merchants who do not participate in the Mastercard® Identity Check™ process?

Yes, this is possible as the Mastercard® Identity Check™ procedure is not mandatory if the merchant's payment service provider (acquirer) is not established in the European Economic Area. Therefore, you will not be asked for approval via app or mobileTAN at these merchants.

24. What should I do if I don't see an Identity Check™ prompt window when shopping online?

Make sure you're using a card for payment that you've registered in the TransactVerify app.

Make sure that any software on your mobile device that prevents input windows from appearing is disabled.

25. I don't automatically receive a message with the payment details I need to confirm after making a purchase with the TransactVerify app. What can I do?

If you allow the "TransactVerify" app to send you notifications in the settings of your mobile device, you will usually automatically receive a push notification. If you do not allow this, you will have to open the app during the payment process and can then approve the payment in the app.

26. What happens if the smartphone has no Internet reception (e.g. airplane mode, roaming function switched off, no Wi-Fi, etc.) and I want to use the "TransactVerify" app?

In this case, the app offers the option of generating a one-time password (OTP) offline, which you can then enter in the browser. Please follow the instructions in the shopping window of your online shop. You will be asked to generate a one-time password in the app and enter your PIN for the app. The password generated by the app can then be entered in the shopping window.

27. My smartphone does not recognize my fingerprint (or my face when Face ID is active) despite repeated attempts. What can I do?

An error message appears when Touch ID/Fingerprint or Face ID cannot be read by the device after multiple attempts.

Android devices usually allow five attempts. After that, the fingerprint scanner can be locked for 15 seconds. You will receive the error message "Identification failed" on your device. iOS devices allow three attempts. You will receive the error message "Identification failed" on your device. This error message also appears when you cancel scanning your fingerprint/face.

Alternatively, you can then use the PIN you chose during registration.

28. What is the list of trusted traders ("whitelist")?

With each online payment, you have the option of adding the merchant to your personal list of trusted merchants for future payments ("whitelist") and storing this list with your card issuer. To do this, click on the corresponding checkbox that will be displayed to you when shopping. For future payments at this merchant, the card issuer can then refrain from authentication. This will make future purchases easier for you.

D) About "eStatement" (card statements)

29. What do I do if I see a transaction on my card statement that I didn't make?

If you see one or more transactions that you have not made, you should immediately contact the cardholder service of your card issuer (Tel. +49-69-7933-1910), complain about the card transaction and have the card blocked.

30. How long are the statements available?

From the time the respective card statement is created, it can be accessed via the app for 12 months.

31. I can't open my monthly card statements. Why?

Check if you have a PDF reader. On iOS devices, this is installed by default. On Android devices, this must be installed manually in order to download statements.

32. How do I know when a new card statement is available for me?

You will not receive a separate notification when new card statements are available. Therefore, please log in to the app regularly. You'll see at a glance if new card statements are available for you.

33. What do I do if I have a question about a statement?

You should then contact the card issuer directly. Some card issuers have a special email link on their electronic statement for billing questions. This allows you to easily ask your question via email.

E) Information on how to view transactions

34. Where can I find more details about a payment (transaction)?

Each transaction can be selected individually to get a detailed view.

35. How can I find a specific transaction?

The search function can be used to search for individual transactions by entering text.

36. How long are transactions available?

Information on transactions can be accessed via the app for three months.

F) Information about Alert Service

37. What does the functional area Alert Service include?

When a payment (transaction) is made with a card registered in the app, you will receive a push notification. This requires activation via the operating settings of your mobile device.

38. How can I turn off notifications about transactions made?

You can deactivate the receipt of push notifications via the operating settings of your mobile device.

Please note that if you deactivate the receipt of push notifications, you will no longer receive any information about payments to be approved via Mastercard® Identity Check™ (3D Secure). However, the function is still available within the app. You must therefore open the app to be able to approve payments using 3D Secure.

G) Administration

39. I got a new smartphone and have installed the "TransactVerify" app on my old smartphone. What do I have to do?

If you have access to both smartphones, you can transfer the existing registration to the new device. On the new device, start the registration process by entering your card number. Then follow the instructions of the app.

If you no longer have access to your previous smartphone, register again. Start the registration in the new app by entering your card number and order a new identification code in the next step. Follow the app's other instructions.

40. How can I deactivate this service?

You can reset the app. Please note that at merchants for whom Mastercard® Identity Check™ is generally mandatory, you will no longer be able to authenticate yourself using the "TransactVerify" app for an online payment without registering again.

41. Can I log in to TransactVerify again or reactivate the feature?

Simply register again. You can then use the service again immediately.

H) Security and privacy

42. What personal data is processed for Mastercard® Identity (3D Secure) Check™ in connection with the app?

In the privacy policy, you will find information on what data is processed in connection with the app, for what purposes, who is the recipient of your data, how long the data will be stored and other information. The privacy policy can be accessed via the app. It complements the data protection information of your card issuer.

43. Which company stores this data?

The card issuer has commissioned First Data GmbH, with its business address in Bad Homburg, Germany, as its service provider to operate Mastercard® Identity Check™, or First Data GmbH is the card issuer itself. First Data GmbH uses Nectetera AG, based in Zurich, Switzerland, as a subcontractor ("Nectetera").

44. What are the privacy and data security terms and conditions for Nectetera for Mastercard® Identity Check™ (3D Secure)?

Registration for Mastercard® Identity Check™ (3D Secure) takes place directly with Nectetera, where your data from the registration process is stored. Nectetera runs the 3D Secure server and tells the merchant if the authentication process was successful.

For Switzerland, the European Commission has issued an adequacy decision on data protection law, i.e. Nectetera has an adequate level of data protection within the meaning of the General Data Protection Regulation (GDPR). First Data GmbH has also agreed the EU standard contractual clauses on data protection with Nectetera.

For more information, please check the privacy policy of the TransactVerify app

45. How secure is the data transfer from my internet browser to Nectetera?

The transmission of the data is of course encrypted. The transmission is secured with TLS 1.2. TLS 1.2 is the highest standard for website encryption currently used in practice.