Procedural notes for the "TransactVerify" app

The following " TransactVerify" app "Procedural notes" provide important legal information and describe the registration as well as the functionalities of the TransactVerify app ("App"). The procedural notes are supplemented by a user guide, FAQ (Frequently Asked Questions) and privacy policy, which can be accessed via the app.

Important legal information

Please note the following important legal notices:

1. Use of the "TransactVerify" app as part of the card contract with the card issuer

1.1 Accessing and using the app does not create a contractual relationship between you and the provider of the app (First Data GmbH (“First Data”) - see Imprint). Rather, the use of the app is part of the contract (“card contract”) concluded for the card with the issuer of your card, a (credit) institution (“card issuer”). Depending on the card issuer's offer, a card is defined as a card with a plastic body (“physical card”), a data record without a plastic body and without a personal identification number (PIN) (‘virtual card’) or a digital card based on a physical or virtual card for storage in an app application for card payments on a mobile device (e.g. smartphone, tablet, smartwatch or wearable).

1.2 Accordingly, First Data assumes no responsibility or liability towards you arising from the operation of the App. Rather, First Data's responsibility and liability are regulated in the card issuer's contract with First Data (if First Data is the card issuer's service provider) or in the card contract (if First Data itself is the card issuer).

1.3 In the event of contradictions between the contractual agreements of the card contract (e.g. General Terms and Conditions) and these procedural notes, the contractual agreements of the card contract shall take precedence.

2. Authorization to access and use the app

2.1 You are only authorized to access and use the App if you are the cardholder of a card for which the card issuer offers you the App for use and if the card issuer uses First Data as a service provider or if First Data itself is the card issuer.

2.2 Natural persons in accordance with section 2.1 may access and use the App. They shall be granted the revocable, non-exclusive, non-transferable and limited right to access and use the App and the content contained therein.

2.3 The card issuer can switch off the operation of the app at any time and provide you with an alternative procedure.

3. Due diligence requirements and precautions

When registering and using the app, please be sure to observe the due diligence requirements and precautions for users of the app. These can be found under "Authorization of Internet Payments via 3D Secure for Internet Payments", under "Due Diligence Requirements and Precautions".

4. App availability

Unrestricted usability and availability of the app is not guaranteed. Restrictions on usability and availability are possible for technical reasons, such as malfunctions or maintenance work, or for reasons beyond the control of the operator of the app.

5. Service provider

The card issuer uses service providers in connection with the operation of the app within the framework of the card contract and provides them with the necessary data. Further information can be found in the privacy policy.

6. Fee for using the app

Whether your card issuer charges a fee for individual or all of the app's functionalities is regulated in your card contract.

7. Costs for mobile phone or internet providers; Roaming costs for use abroad

When loading and using the app, fees may be charged by the mobile phone or internet provider you use. This can also include roaming costs if you are abroad. You are responsible for the contract for this as well as the associated costs of the provider (e.g. for roaming costs incurred abroad).

App functionalities, user guide and FAQ

1. Functionalities and possible uses of the app

1.1 The App enables authentication for payment transactions on the Internet ("**Internet Payments**") by means of Mastercard® Identity Check™) ("**3D Secure**."). 3D Secure is a process that aims to make online payments more secure by verifying your identity during the checkout process. Authentication allows you to identify yourself as an authorized cardholder to the card issuer. 3D Secure thus helps to prevent fraudulent transactions.

1.2 Under certain circumstances, the card issuer may offer other methods as an alternative to the app authorization for Internet payments using 3D Secure (e.g. authentication by entering a mobile TAN received on the mobile device), but these are not carried out via the app. Please contact the card issuer for more information.

The 3D Secure functionality is always activated when registering in the app.

1.2 The app also allows you to view and download card statements for cards registered in the app (functional area "**eStatements**"). This is an optional additional functionality and requires that the card issuer offers the functionality, that the card in question has been registered in the app and that the functionality has been activated in the app.

1.3 The app also allows you to view information about payments made with cards registered in the app (functional area "**Transactions**"). This is also an optional additional functionality and requires that the card issuer offers the functionality and that the card in question has been registered in the app.

1.4 The app also allows you to receive messages in the app when payments have been made with a card registered in the app (functional area "**Alert Service**"). This is also an optional additional functionality and requires that the card issuer offers the functionality, registers the card in question in the app and activates the receipt of messages in the operating settings of the mobile device.

1.5 Finally, the app allows you to view the card limit and the amount of cards registered in the app that is still possible for the month in question (functional area "**Card balance**“).

2. The **User Guide** gives detailed information about the functionalities and functionality of the app. The **FAQ**, which can also be accessed in the app, answer frequently asked questions.

3. The app is designed for use on smartphones. The use on tablets is possible, but is not recommended due to special features in the display (only upright).

Registration in the app

1. The use of the app requires the registration in the app. The registration is done via 3D Secure.

2. First, you choose an authentication method for 3D Secure. With the help of the method you have chosen, the card issuer will be able to authenticate you for Internet payments in the future.

   2.1 In any case, you must choose a four- to six-digit PIN. To do this, set a PIN in the app. You will also need this PIN if you chose biometric recognition to confirm internet payments (see section 2.2). You can use the PIN if Face ID or fingerprint cannot be read.

   2.2 Alternatively, you can chose the biometric recognition. The app supports Face ID and Touch ID/fingerprint recognition. If you have selected biometric recognition in the app, the app will ask the mobile device whether biometrics have been set up in the device. If the end device of the app gives the feedback that biometrics has not yet been set up, the app informs you about this. Therefore, you can only choose biometric recognition if you have enabled Face ID or Touch ID/fingerprint recognition in the mobile device's settings.

   Once the device has successfully captured your Face ID or fingerprint, the device notifies the app that the biometrics were correct. The type of biometric recognition that you have defined in the settings of the mobile device, is then used for authentication within 3D Secure.

3. Then enter your card number in the app under the menu item "+ Add credit card", either manually or by scanning the card with the Card-Scanner. If the card number is entered by scanning the card, you will need to agree to use your mobile device's camera in the app.

4. The app establishes a link between the card number entered in the app and the number of the app installation on the mobile device ("**emCertID**“).

5. You must then identify yourself as part of the registration process. To do this, you first need an identification code. To receive the identification code, choose either SMS, a 1-cent transfer to the settlement account agreed between you and the card issuer, or a letter. Your card issuer may only offer some of these methods.

   If you wish to receive the identification code by SMS, you must then enter the last four digits of your account number, the expiry date of the card, your date of birth and your mobile phone number into the app. The mobile phone number must be identical to the one you gave to your card issuer, e.g. in the card application.

6. After receiving the identification code via the method, you have chosen (see section 5.), enter the identification code in the app.

7. There is also the option of offline authentication for internet payments as an alternative to the authentication methods described in section 2. A separate registration in the app is not required for this. This method of authentication is used at merchants or acceptance points that offer offline authentication by scanning the QR code displayed on the merchant's or acceptance point's website with the app during the payment process.

8. If the app needs to be reinstalled, e.g. due to a change of mobile device, or if the PIN for the approval of payments has been forgotten (see section 2.1), a full re-registration must be performed.

9. You can register multiple cards in the app. This also applies to cards from several card issuers, provided that the card issuers use First Data as a service provider or First Data itself is the card issuer.

Authorization of Internet Payments via 3D Secure for Internet payments

1. If your card issuer requires authentication using 3D Secure for an online payment,

1.1 The card issuer sends you a message to your mobile device using the card number and emCertID. This message contains the last four digits of your card number, the name of the merchant or acceptance point where the internet payment is made, and the date, time and amount of the internet payment.

1.2. Then please open the app.

a) On the confirmation page that appears to you, confirm the payment with the payment details. To do this, use the "Confirm" button.

b) In addition, you use the recognition method selected by you as part of the registration in the app for approval.

You either enter the PIN that you have set.

Or you can use the type of biometric recognition you specified (Face ID or Touch ID/fingerprint recognition). If you confirm the internet payment through biometric recognition, the biometric recognition will be performed by your mobile device, and your mobile device will inform the app whether the authentication was successful or not.

c) As an alternative to point b), you can confirm the payment by scanning the QR code displayed on the merchant's website (acceptance point), if you have selected the offline authorization on the merchant's website. To do this, open the QR code scanner in the app and scan the QR code displayed.

1.3 If you do not want to confirm the online payment, you can decline the payment. To do this, use the "Reject" button. This is especially the case if the payment details do not correspond to the data you expected or the payment was not made by you at all

2. Blocking of the card for the 3D Secure procedure

The card issuer may block the card for the 3D Secure procedure if there are objective reasons in connection with the security of the 3D Secure procedure or if there is a suspicion of fraudulent use of the 3D Secure procedure. To remove the block, please contact your card issuer via the communication channels provided to you by the card issuer.

2. Due Diligence Requirements and Precautions

3.1 Please take precautions to protect your mobile device and the authentication elements (see Section 1.2 b) from unauthorized access. Otherwise, there is a risk that they will be misused for the 3D Secure procedure and that unauthorized Internet payments with the card will occur.

3.2 Please protect in particular the mobile device linked to the app from misuse. Ensure that other persons cannot use the app on the mobile device, and deactivate the application on the mobile device before giving up possession of the mobile device (e.g. by selling or disposing of the mobile phone).

3.3 Please compare the details of the internet payment submitted during the payment process for authentication within the 3D Secure procedure with the data you have intended for payment. In the event of discrepancies, cancel the payment and inform the card issuer immediately via the communication channels communicated to you by the card issuer. Likewise, inform the card issuer immediately if you receive a request to confirm a payment transaction that has not been made by you.

3.4 Please minimize the risk of unauthorized access to your mobile device, by taking appropriate protective measures (e.g. a password-protected access lock). Also, make sure that if you use biometrics instead of a password to access your mobile device, only your own biometric feature is stored on the device.

3.5 Keep the operating system of the mobile device up to date and do not change the administrator rights or remove usage restrictions set by the manufacturer (jailbreaking, rooting).

3.6 The card issuer will never ask you to provide your registration details by email, text message or phone call.

Retrieval of card statements (functional area "eStatements") and

View Payments (Transactions functional area)

1. If the card issuer offers you the "eStatements" function, you have registered the card in question in the app (see "Registration in the app") and you have also activated the eStatements function in the app (button "eStatements"), you can view your card statements in the "eStatements" functional area and download them as pdf documents.

2. You can view card statements for multiple cards in the app, as long as you have registered the cards in the app. This also applies to cards from several card issuers, provided that the card issuers use First Data as a service provider or First Data itself is the card issuer.

3. Card statements are made available in the app once a month, provided that payments have been made with the card in question. It is provided in pdf format. There is no notification about new card statements in the app. In the period between two card statements, you can view the transactions in the "Transactions" functional area.

4. Card statements (functional area "eStatements") and the overview of transactions (functional area "Transactions") contain all payments made with the card in question, regardless of which payments were made with the card, e.g. Internet payments, payments in physical stores or cash withdrawals (e.g. at ATMs).

5. Card statements will be made available in the App for twelve months at a time and transaction information for at least three months at the time these procedural notes are created. After that, they will be automatically deleted without separate notification.
6. Please check the card statements as soon as possible after they have been made available and check them immediately for accuracy. If you have any objections, please contact the card issuer in accordance with the specifications in the card contract.
7. The card contract determines whether the card issuer will continue to provide you with card statements by letter or in any other way in addition to making them available in the app, or whether this is only the case under certain conditions as long as you can access the card statements in the app.
8. You can deactivate the eStatements functionality in the app at any time. You will then receive your card statement by letter.
9. Payment information in the functional area “Transactions” may include additional information about the merchant or acceptance point where a registered card was used to make payments. However, this presupposes that this information is provided by the Mastercard card organization . No responsibility can be assumed for the content of this information.

Receiving messages about payments made with registered cards (Alert Service functional area)

1. "Alert Service" is an optional functionality. It requires that the card issuer offers you the "Alert Service" function, that you have registered the card in question in the app (see section "Registration in the app") and that you have also activated the receipt of messages in the operating settings of your mobile device.
2. Via "Alert Service", you will always receive a message in the app after a payment has been made with a registered card. This applies to all payments made with the card in question, regardless of whether they are e.g. internet payments, payments in physical stores or cash withdrawals (e.g. at ATMs).
3. The notification is usually sent directly after the internet payment. If the (mobile) device is not accessible (e.g. no internet connection), there may be delays in the receipt of messages or it is possible that the notification does not arrive at all. This cannot be influenced by the card issuer.
4. For security reasons, only the last 4 digits of the card number are transmitted when a notification is made. The first and last name of the card user are not mentioned. The notification contains information about the merchant and the amount of the payment.
5. You can receive messages for multiple cards as long as you have registered the cards in the app. This also applies to cards from several card issuers, provided that the card issuers use First Data as a service provider or First Data itself is the card issuer.
6. You can deactivate the "Alert Service" functionality at any time by deactivating the receipt of messages in the operating settings of your mobile device.
7. If you receive a message about an internet payment that has not been made by you, please contact your card issuer immediately via one of the communication channels provided to you by your card issuer.
8. The notification is purely informative. Only the information on your card issuer's card statement is legally binding with regard to Internet payments.

Card limit display (Card Balance functional area)

1. In the "Card balance" functional area of the app, you can also view the limit (credit limit) and the available limit (i.e. the limit that has not yet been used for payments (e.g. internet payments, over-the-counter payments or cash withdrawals)) (credit limit) for the relevant card.

2 The "Card balance" functionality requires that you have registered the card in question in the app (see "Registration in the app").