Information pursuant to Sections 5, 7 and 8 of FernFinG:

1. Company description

- Name and address:
  PayLife Service Center
  BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft ("bank" for short),
  Wiedner Gürtel 11, 1100 Vienna, Austria

- Main business activity:
  Banking transactions within the meaning of Sect 1 of BWG, the Austrian Banking Act, and, in particular, the implementation of cashless payment transactions

- Company-register number/Company-register court:
  FN 205340x , Handelsgericht Wien (Vienna Commercial Court)

- Competent supervisory authority:
  Financial Market Authority (FMA), Otto-Wagner-Platz 5, 1090 Vienna, Austria

2. Description of the financial service

Key features of the financial service:
The bank offers the authentication method 3D Secure for the secure handling of payments on the Internet for which you can register by submitting certain data. In this process, a payment is made after the entry of certain data available or generated in the system that are suitable for identifying you.

Your instruction (e.g. entry of a password and an additional authorization feature by way of a mobileTAN or a biometric feature etc. in the framework of the secure procedure) will make your payment order irrevocable. The implementation of your payment order will be settled between your merchant and their payment service provider.

3. Total price that you owe for the financial service

(1) You are not obliged to pay a fee to the bank for participation in the 3D Secure.
(2) For the services rendered by the bank that you use by using 3D Secure you shall pay the fees that the bank has paid to the merchant for you due to the business transactions concluded between you and the merchant concerning goods and services. These fees are debited from your account by way of the direct-debit procedure, with these fees being agreed in the agreement underlying the respective service and concluded between the bank and the customer, e.g. in the account contract.
(3) The customer shall bear the costs for using distance-communications media (e.g. smartphone) himself/herself.

4. Note concerning right to rescind the contract pursuant to Sect 8 of FernFinG

Pursuant to Sect 8 of FernFinG, you shall be entitled to rescind the concluded agreement on your participation in 3D Secure within 14 days. The rescission period shall begin on the day of online registration pursuant to Clause 3 of the Special terms for cashless payments on the Internet using 3D Secure (i.e. the day of contract conclusion).

If you want to make use of your right to rescind the contract pursuant to Sect 8 of FernFinG, you are obliged to submit your explicit written rescission to PayLife Service Center, Wiedner Gürtel 11, 1100 Vienna, Austria. If you fail to use such right to rescind the contract within 14 days starting from contract conclusion, the agreement concluded with you on the participation in 3D Secure shall be valid for an indefinite period of time, yet no longer than the underlying credit card agreement.

Pursuant to Sect 8 Para 5 of FernFinG, the performance of the contract may be started within the rescission period only upon your express consent. In such a case, we are entitled to charge the agreed fees and compensation for efforts for services that we provided before the expiry of the rescission period that you are entitled you pursuant to Sect 8 of FernFinG.

5. Termination

You can block access to the authentication method 3D Secure at any time or change your 3D Secure password yourself. The bank shall be entitled to block 3D Secure if such is justified by objective security reasons or if non-authorized or fraudulent use is suspected.
Moreover, the bank shall be entitled to dissolve the credit card agreement underlying the agreement on participation in 3D secure by observing a two-month notice period and for good cause at any time.

6. Applicable law and place of jurisdiction

The agreement on participation in 3D Secure as well as the precontractual relationships shall be based on Austrian law. The general place of jurisdiction in Austria applicable for your law suits against the bank and for the law suits initiated against you shall also remain to be valid if you relocate to another country after contract conclusion and Austrian court decisions are enforceable in such country.

7. The information pursuant to Sects 5 and 8 of FernFinG

as well as the contractual terms underlying this contract are communicated to you in the German language. For the duration of the contract, the bank will communicate with you in German.

8. Information on legal orders pursuant to Sect 5 Para 1 Subpara 4 of FernFinG

For the out-of-court settlement of disputes in connection with certain customer complaints in the banking industry, the "Gemeinsame Schlichtungsstelle der Österreichischen Kreditwirtschaft" (Joint Conciliation Board of the Austrian Banking Industry), Wiedner Hauptstrasse 63, 1045 Vienna, Austria, was set up. You can file a complaint with this conciliation board either in writing or electronically (e-mail to: office@bankenschlichtung.at) by briefly stating the facts of the case and by attaching the required documents.

To make them easier to read, the Special Terms and Conditions for participation in 3D Secure for PayLife credit cards are not worded in a gender-specific manner and apply equally to all genders.

1. Special Terms and Conditions

The Special Terms and Conditions at hand for participation in 3D Secure for PayLife credit cards ("STC" for short) shall govern the handling of payments with PayLife credit cards by using 3D Secure. These STC shall apply to the extent that their applicability has been agreed. They shall supplement the General Terms and Conditions for PayLife credit cards ("GTC" for short) agreed upon and pertaining to the credit card agreement concluded between BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft ("bank" for short) and the cardholder on the issuance of his/her PayLife credit card ("card" for short).

2. Definitions

2.1. 3D Secure
The authentication method 3D Secure is a secure system used for online payments fulfilling the requirement of strong customer authentication.

2.2. "3D Secure password": Mastercard Identity Check or Visa Secure password
The 3D Secure password is the secret word (combination of characters) defined by the cardholder when registering for the authentication method 3D Secure. Such secret word is designated as "Mastercard Identity Check" at Mastercard and as "Visa Secure" password at Visa and serves the issuance of payment orders on the Internet.

2.3. Mobile Transaction Number ("mobileTAN" for short)
The mobileTAN is a one-time transaction number sent to the mobile phone number disclosed by the cardholder for the purpose of delivering the mobileTAN via text message. Constituting an additional security feature on top of the 3D Secure password, the mobileTAN serves the issuance of a payment order on the Internet. Entry of a mobileTAN is also required when registering for the authentication method 3D Secure.

2.4. PayLife secCheck app
The PayLife secCheck app is an application (for the iOS and Android operating systems) provided by the bank and serves the passing of amounts for payment on the Internet by way of a biometric security feature (e.g. fingerprint, face recognition) or app PIN. In the course of registration in the PayLife secCheck app, the cardholder selects a biometric security feature and a secret code (app PIN) for passing amounts for payment on the Internet. If the mobile end device does not have any functions for checking the biometric security features (e.g. fingerprint sensor), the cardholder shall select a secret code (app PIN).
The cardholder may change the app PIN at any time at my.paylife.at.

2.5. Authentication code
The authentication code is a code that is generated in the case of strong customer authentication within the meaning of Delegated Regulation (EU) 2018/389 and that is dynamically linked to the step that is to be authorized (e.g. to the order to be authorized or to the card holder's declaration of intent). The mobileTAN constitutes such authentication code.

2.6. Strong customer authentication
As strong customer authentication shall be deemed the procedure for strong customer authentication governed in Delegated Regulation (EU) 2018/389. Strong customer authentication is based on (at minimum) two factors falling into the categories of knowledge (e.g. password), possession (e.g. smartphone) and inherence (e.g. fingerprint, face recognition), and prompts the generation of an authentication code.

3. Registration for the authentication method 3D Secure

3.1. The prerequisite for using 3D Secure is the cardholder's registration for 3D Secure. Registration is performed in the Online Services ("my.paylife.at"). On the www.paylife.at/3dsecure website, the registration process is explained to the cardholder. For cardholder identification in the course of registration for the 3D Secure procedure, a mobileTAN is sent to the cardholder via text message to the mobile phone number disclosed by him/her for delivering a mobileTAN

3.2. In the course of registration, the cardholder is obliged to define personal identification features himself/herself:
- 3D Secure password (Mastercard Identity Check or Visa Secure password) or
- By using the PayLife secCheck app: a biometric security feature (e.g. fingerprint) and the app PIN

The cardholder may change his/her personal identification features at any time himself. Should the cardholder forget the password selected by himself/herself, he/she can create a new 3D Secure password or a new app PIN in the Online Services ("my.paylife.at").
In the course of registration for the authentication method 3D Secure, the cardholder is required to disclose his/her e-mail address.
Taking the technical precautions for providing proper text-message reception and the resulting costs shall be the responsibility of the cardholder.

4. Making payments with 3D Secure

The cardholder may perform Internet payment transactions either with the 3D Secure password defined by himself and a mobileTAN or by using the PayLife secCheck app using his biometric security feature or the app PIN.

5. Due-diligence obligations and security measures recommended when using 3D Secure

5.1. Compliance and legal consequences
Every cardholder shall be obliged to comply with the due-diligence obligations contained in Clause 5.4. In addition, cardholders shall be obliged to comply with the security measures recommended under Clause 5.5. The bank advises cardholders that are deemed as consumers to comply with the recommended security measures without consumers being obliged to comply with them. Pursuant to Clause 6, violation of these obligations may lead to damage compensation obligations incumbent on the cardholder or to abrogation or abatement of his/her damage compensation claims vis-à-vis the bank.

5.2. Obligation to secrecy and obligation to blockage

5.2.1 The cardholder shall be obliged to keep his/her 3D Secure password and the app PIN secret and must not pass such on to unauthorized third parties; the e-mail address shall be excepted from the obligation to secrecy. Passing on the personal security features to service providers triggering payments and account information service providers shall, however, be admissible, to the extent that such is required in order for them to be able to provide their services to the cardholder.

5.2.2. The cardholder shall be obliged to display the utmost amount of care when safekeeping and using his/her 3D Secure password and the app PIN in order to prevent misuse. The cardholder shall, in particular, ensure that his/her 3D Secure password and the app PIN are not spied out while they are used; s/he must also not store or note it down electronically – e.g. in an app used for taking notes – in his/her mobile end device on which s/he has installed the PayLife secCheck app.

5.2.3. When losing the 3D Secure password and/or the app-PIN and also when the cardholder becomes aware of the misuse or any other non-authorized use of the authentication method 3D Secure, the cardholder shall be obliged to immediately prompt blockage of the authentication method 3D Secure.

5.2.4. In the event of loss or theft of the cardholder's mobile end device on which s/he has installed the PayLife secCheck app the cardholder shall immediately prompt blockage of the authentication method 3D Secure.

5.3. Due-diligence obligations for blockage of the end device and applicable during installation

5.3.1. The cardholder shall be obliged to block the access to use of the mobile end device on which the PayLife secCheck App is installed and/or block access to data stored on such device

for non-authorized parties when s/he does not use the end device.

5.3.2. The cardholder may install the PayLife secCheck app exclusively from the Apple app store or Google Play store.

5.4. Due-diligence obligations regarding orders

5.4.1. Payment approval via mobileTAN
The data displayed in the mobileTAN shall be checked for correctness by the cardholder prior to use. Only if the displayed data match the intended payment order may the mobileTAN be used for approving orders.

5.4.2. Payment approval via PayLife secCheck app
The data transmitted to the PayLife secCheck app shall be checked for correctness by the cardholder prior to payment release. Only if the displayed data match the intended payment order may the payment be approved.

5.5. Recommended security measures when using the authentication method 3D Secure

5.5.1. The cardholder is advised to change the 3D Secure password and the app PIN on a regular basis, yet every two months at the latest, without being prompted to do so.

5.5.2 The cardholder is advised to immediately prompt blockage of 3D Secure if there is reasonable suspicion that the password and/or the app PIN have come to the notice of unauthorized third parties, or if there are other circumstances possibly enabling an unauthorized third party to perform misuse.

5.5.3. The cardholder is advised to protect his/her mobile end device on which s/he receives the mobileTAN and/or on which the PayLife secCheck app has been installed against risks emanating from the Internet, and, in particular, to use up-to-date virus protection and to always keep such up-to-date, and to perform security updates of the mobile device's operating system.

6. Cardholder liability

6.1. The cardholder shall be liable for the entire damage resulting from a non-authorized online payment that s/he has caused to the bank due to willful or grossly negligent violation of the due-diligence obligations under Clause 5. If the cardholder has violated the due-diligence obligations under Clause 5 neither in a willful nor in a grossly negligent manner, it shall be, in particular, the type of the personalized security features as well as the special circumstances under which misuse of the card has been performed that shall be taken into account in the event of claim sharing, if any, between the cardholder and the bank.

6.2. If it was not possible for the cardholder to become aware of the loss or theft of his/her personal identification features or of the misuse of his/her card prior to payment, s/he shall, in deviation from Clause 6.1., not be liable in the event of slightly negligent violation of the due- diligence obligations pursuant to Clause 5. The cardholder shall also not be liable in the event of slightly negligent violation of the due- diligence obligations pursuant to Clause 5 if the bank has caused the loss of the personal identification features.

6.3. In deviation from Clause 6.1., the cardholder shall not be liable if the bank has not required any strong customer authentication in the event of misuse or any other non-authorized use of the card in the course of an online payment (i.e. the online payment has been performed without using the authentication method 3D Secure). If a non-authorized online payment was enabled by the cardholder with fraudulent intent, the cardholder shall be liable irrespective of the bank having required strong customer authentication or not.

6.4. The cardholder shall not be liable if the damage results from non-authorized use of the card during an online payment after the blockage has been ordered pursuant to Clause 7 unless the cardholder has acted with fraudulent intent.

7. Blockage of the authentication method 3D Secure

7.1. Automatic blockage
For security reasons, the authentication method 3D Secure will be blocked by the bank after the personal security features have been entered incorrectly five times in a row. As long as blockage is active, the cardholder cannot give any payment orders using the authentication method 3D Secure.

7.2. Blockage by the cardholder
The cardholder can perform blockage of 3D Secure due to the five-time consecutive incorrect entry of the security features himself/herself or have it blocked at +43 (0)5 99 06-6220.

7.3. Blockage by the bank

7.3.1. The bank is entitled to block the authentication method 3D Secure for the cardholder in the event of objective security reasons justifying such or in the event of non-authorized or fraudulent use.

7.3.2. The bank will inform the cardholder of blockage of the authentication method 3D Secure and of the reasons for such blockage to the extent possible prior to, but, at the latest, immediately after blockage, to the extent that blockage notification or the reasons for the blockage do not violate a court or administrative-authority order and/or would be contrary to Austrian or community-law legal norms or objective security considerations.

7.4. Notification and deactivation of blockage

7.4.1. Before a blockage becomes permanent, the cardholder will receive a warning.

7.4.2. The bank will deactivate blockage pursuant to 7.3. as soon as the reasons for blockage are no longer existent. The bank will inform the cardholder immediately of blockage deactivation.

7.4.3 The cardholder can order deactivation of the blockage at +43 (0)5 99 06-6220. The cardholder can also deactivate the blockage himself/herself in the Online Services ("myPayLife") by setting a new password.

8. Changes of the Special Terms and Conditions for participation in 3D Secure for PayLife credit cards

8.1. Changes of the Special Terms and Conditions for participation in 3D Secure for PayLife credit cards will be offered to the cardholder by the bank at minimum two months before the proposed date of their entry-into-force; in this process, the terms affected by the change offer and the proposed changes to these terms are displayed in a comparison attached to the change offer (referred to as "comparison" in the following). The change offer will be communicated to the cardholder. The cardholder's consent is deemed to have been granted if the bank does not receive any written objection or any electronically-declared objection in the manner agreed with the cardholder (e.g. per e-mail or via the virtual mailbox in the myPayLife service portal).
In the change offer, the bank will inform the cardholder that his/her silence due to the omission of a written objection or an electronically- declared objection in the manner agreed with the cardholder shall be deemed as consent to the changes, and that the cardholder, in his/her capacity as consumer, is entitled to cancel the agreement on participation in 3D Secure as well as the credit card agreement before the entry-into-force of the changes without notice and free-of-charge. Morever, the bank will publish the comparison as well as the complete version of the new terms on its website and send the complete version of the new terms to the cardholder upon the latter's request; also to this fact, the bank will draw attention in the change offer.

8.2. The cardholder may be notified of the proposed changes in any way agreed with him/her. As such form shall also be deemed the communication of the change offer including the comparison to the e-mail address announced to the bank by the cardholder or to the virtual mailbox in the myPayLife service portal, with the cardholder being notified of the change offer being available in his/her virtual mailbox in the manner agreed with him/her (push message, text message, e-mail, post or any other agreed form).

8.3. Any changes of these terms shall be confined to objectively justified cases. The following shall be deemed as objective justifications:

(i) if the change is required due to a change of the legal provisions relevant for payment services as well as for the handling of payment services or due to provisions enacted by the Financial Market Authority, the European Banking Supervisors, the European Central Bank or the Austrian National Bank,

(ii) if the change is required due to the development of the case law relevant for payment services as well as for the handling of payment services,

(iii) if the change enhances the security of banking operation or the security of handling the business relationship with the cardholder via participation in 3D secure,
(iv) if the change is required for the implementation of technological developments or for the adaptation to new programs for the use of end devices,
(v) if the change is required due to a change in the legal provisions applicable for issuing orders and for submitting declarations concerning the participation in 3D Secure,
(vi) if the change is required due to a change in the legal provisions applicable for the banking transactions that the cardholder can handle via 3D Secure.

The introduction of fees or the changes of agreed fees by way of a change of the STC at hand shall be excluded.

9. Change of cardholder's e-mail address and mobile phone number

The cardholder undertakes to announce any change of his/her e-mail address and mobile phone number to the bank either in writing or per e-mail. This shall not affect the provision under Clause 16. of the GTC.

10. Security notes

10.1. As long as access to the authentication method 3D Secure is blocked, the card cannot be used for payment purposes at Internet merchants to the extent that they offer 3D Secure.
10.2. To prevent risks connected to gaining knowledge of the identification features (in particular of the 3D Secure password) the bank recommends changing them at regular intervals (e.g. each month).
10.3. If the cardholder should suspect that his/her identification features (in particular the 3D Secure password) have come to the attention of third parties, the bank recommends changing the identification features.
10.4. Cardholders are advised to secure access to the use of mobile data terminal devices. In the event of loss or theft of the mobile data terminal device the bank recommends contacting the mobile telephony provider for the purpose of SIM card blockage.
10.5. Please note that the use of passwords on shared computers and mobile data terminal devices (e.g. in an Internet café, in a hotel, at the workplace) enables unauthorized third parties to spy out passwords.
10.6. On the www.paylife.at website, the bank will make available further information on the secure systems as well as security advice under menu item "Service".

11. Duration of contract, cancellation and termination

11.1. The agreement on participation in 3D Secure is concluded for an indefinite period of time.
11.2. The cardholder is entitled to cancel the agreement at any time without having to state any reasons for such and without having to observe a notice period. After receipt of the cancellation, the bank will block access to the authentication method 3D Secure.
11.3. The bank is entitled to cancel the agreement at any time by observing a two-month notice period and without having to state any reasons for doing so.
11.4 The cardholder as well as the bank are entitled to cancel he agreement at any time and with immediate effect in the event of good cause.
11.5 The termination of the agreement shall not affect the credit card agreement unless the cardholder/the bank simultaneously declare the termination of the latter.
11.6 The agreement shall automatically end upon the end of the credit card agreement.

As of September 2019, version of March 2020

To make them easier to read, the Special Terms and Conditions for participation in 3D Secure for PayLife prepaid cards are not worded in a gender-specific manner and apply equally to all genders.

1. Special Terms and Conditions

The Special Terms and Conditions at hand for participation in 3D Secure for rechargeable PayLife prepaid cards ("STC" for short) shall govern the handling of payments with PayLife prepaid cards by using 3D Secure. These STC shall apply to the extent that their applicability has been agreed. They shall supplement the General Terms and Conditions for PayLife prepaid cards ("GTC" for short) agreed upon and pertaining to the prepaid-card agreement concluded between BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft ("bank" for short) and the cardholder on the issuance of his/her PayLife prepaid card ("card" for short).

2. Definitions

2.1. 3D Secure
The authentication method 3D Secure is a secure system used for online payments fulfilling the requirement of strong customer authentication.

2.2. "3D Secure password": Mastercard Identity Check
The 3D Secure password is the secret word (combination of characters) defined by the cardholder when registering for the authentication method 3D Secure. Such secret word is designated as "Mastercard Identity Check" at Mastercard and serves the issuance of payment orders on the Internet.

2.3. Mobile Transaction Number ("mobileTAN" for short)
The mobileTAN is a one-time transaction number sent to the mobile phone number disclosed by the cardholder for the purpose of delivering the mobileTAN via text message. Constituting an additional security feature on top of the 3D Secure password, the mobileTAN serves the issuance of a payment order on the Internet. Entry of a mobileTAN is also required when registering for the authentication method 3D Secure.

2.4. PayLife secCheck app
The PayLife secCheck app is an application (for the iOS and Android operating systems) provided by the bank and serves the passing of amounts for payment on the Internet by way of a biometric security feature (e.g. fingerprint, face recognition) or app PIN. In the course of registration in the PayLife secCheck app, the cardholder selects a biometric security feature and a secret code (app PIN) for passing amounts for payment on the Internet. If the mobile end device does not have any functions for checking the biometric security features (e.g. fingerprint sensor), the cardholder shall select a secret code (app PIN).
The cardholder may change the app PIN at any time via registration website.

2.5. One-time password
The one-time password is a randomly-assigned keyword that serves cardholder verification during registration for the authentication method 3D Secure. In the course of 3D Secure registration process for payment approval via mobileTAN and password, the one-time password shall be replaced by entry of an individually-selected 3D Secure password exclusively known to the cardholder.

2.6. Authentication code
The authentication code is a code that is generated in the case of strong customer authentication within the meaning of Delegated Regulation (EU) 2018/389 and that is dynamically linked to the step that is to be authorized (e.g. to the order to be authorized or to the card holder's declaration of intent). The mobileTAN constitutes such authentication code.

2.7. Strong customer authentication
As strong customer authentication shall be deemed the procedure for strong customer authentication governed in Delegated Regulation (EU) 2018/389. Strong customer authentication is based on (at minimum) two factors falling into the categories of knowledge (e.g. password), possession (e.g. smartphone) and inherence (e.g. fingerprint, face recognition), and prompts the generation of an authentication code.

3. Registration for the authentication method 3D Secure

3.1. The prerequisite for using 3D Secure is the cardholder's registration for 3D Secure. On the www.paylife.at/3dsecure website, the registration process is explained to the cardholder. For cardholder identification in the course of registration for the authentication method 3D Secure, a valid one-time password and a mobileTAN is necessary. During the registration process a mobileTAN is sent to the cardholder via text message to the mobile phone number disclosed by him/her for delivering a mobileTAN.

3.2. In the course of registration, the cardholder is obliged to define personal identification features himself/herself:
- 3D Secure password (Mastercard Identity Check) or
- By using the PayLife secCheck app: a biometric security feature (e.g. fingerprint) and the app PIN

The cardholder may change his/her personal identification features at any time himself. Should the cardholder forget the password selected by himself/herself, he/she can create a new 3D Secure password or a new app PIN via the registration website.
In the course of registration for the authentication method 3D Secure, the cardholder is required to disclose his/her e-mail address.
Taking the technical precautions for providing proper text-message reception and the resulting costs shall be the responsibility of the cardholder.

4. Making payments with 3D Secure

The cardholder may perform Internet payment transactions either with the 3D Secure password defined by himself and a mobileTAN or by using the PayLife secCheck app using his biometric security feature or the app PIN.

5. Due-diligence obligations and security measures recommended when using 3D Secure

5.1. Compliance and legal consequences
Every cardholder shall be obliged to comply with the due-diligence obligations contained in Clause 5.4. In addition, cardholders shall be obliged to comply with the security measures recommended under Clause 5.5. The bank advises cardholders that are deemed as consumers to comply with the recommended security measures without consumers being obliged to comply with them. Pursuant to Clause 6, violation of these obligations may lead to damage compensation obligations incumbent on the cardholder or to abrogation or abatement of his/her damage compensation claims vis-à-vis the bank.

5.2. Obligation to secrecy and obligation to blockage

5.2.1 The cardholder shall be obliged to keep his/her 3D Secure password and the app PIN secret and must not pass such on to unauthorized third parties; the e-mail address shall be excepted from the obligation to secrecy. Passing on the personal security features to service providers triggering payments and account information service providers shall, however, be admissible, to the extent that such is required in order for them to be able to provide their services to the cardholder.

5.2.2. The cardholder shall be obliged to display the utmost amount of care when safekeeping and using his/her 3D Secure password and the app PIN in order to prevent misuse. The cardholder shall, in particular, ensure that his/her 3D Secure password and the app PIN are not spied out while they are used; s/he must also not store or note it down electronically – e.g. in an app used for taking notes – in his/her mobile end device on which s/he has installed the PayLife secCheck app.

5.2.3. When losing the 3D Secure password and/or the app-PIN and also when the cardholder becomes aware of the misuse or any other non-authorized use of the authentication method 3D Secure, the cardholder shall be obliged to immediately prompt blockage of the authentication method 3D Secure.

5.2.4. In the event of loss or theft of the cardholder's mobile end device on which s/he has installed the PayLife secCheck app the cardholder shall immediately prompt blockage of the authentication method 3D Secure.

5.3. Due-diligence obligations for blockage of the end device and applicable during installation

5.3.1. The cardholder shall be obliged to block the access to use of the mobile end device on which the PayLife secCheck App is installed and/or block access to data stored on such device for non-authorized parties when s/he does not use the end device.

5.3.2. The cardholder may install the PayLife secCheck app exclusively from the Apple app store or Google Play store.

5.4. Due-diligence obligations regarding orders

5.4.1. Payment approval via mobileTAN
The data displayed in the mobileTAN shall be checked for correctness by the cardholder prior to use. Only if the displayed data match the intended payment order may the mobileTAN be used for approving orders.

5.4.2. Payment approval via PayLife secCheck app
The data transmitted to the PayLife secCheck app shall be checked for correctness by the cardholder prior to payment release. Only if the displayed data match the intended payment order may the payment be approved.

5.5. Recommended security measures when using the authentication method 3D Secure

5.5.1. The cardholder is advised to change the 3D Secure password and the app PIN on a regular basis, yet every two months at the latest, without being prompted to do so.

5.5.2 The cardholder is advised to immediately prompt blockage of 3D Secure if there is reasonable suspicion that the password and/or the app PIN have come to the notice of unauthorized third parties, or if there are other circumstances possibly enabling an unauthorized third party to perform misuse.

5.5.3. The cardholder is advised to protect his/her mobile end device on which s/he receives the mobileTAN and/or on which the PayLife secCheck app has been installed against risks emanating from the Internet, and, in particular, to use up-to-date virus protection and to always keep such up-to-date, and to perform security updates of the mobile device's operating system.

6. Cardholder liability

6.1. The cardholder shall be liable for the entire damage resulting from a non-authorized online payment that s/he has caused to the bank due to willful or grossly negligent violation of the due-diligence obligations under Clause 5. If the cardholder has violated the due-diligence obligations under Clause 5 neither in a willful nor in a grossly negligent manner, it shall be, in particular, the type of the personalized security features as well as the special circumstances under which misuse of the card has been performed that shall be taken into account in the event of claim sharing, if any, between the cardholder and the bank.

6.2. If it was not possible for the cardholder to become aware of the loss or theft of his/her personal identification features or of the misuse of his/her card prior to payment, s/he shall, in deviation from Clause 6.1., not be liable in the event of slightly negligent violation of the due- diligence obligations pursuant to Clause 5. The cardholder shall also not be liable in the event of slightly negligent violation of the due- diligence obligations pursuant to Clause 5 if the bank has caused the loss of the personal identification features.

6.3. In deviation from Clause 6.1., the cardholder shall not be liable if the bank has not required any strong customer authentication in the event of misuse or any other non-authorized use of the card in the course of an online payment (i.e. the online payment has been performed without using the authentication method 3D Secure). If a non-authorized online payment was enabled by the cardholder with fraudulent intent, the cardholder shall be liable irrespective of the bank having required strong customer authentication or not.

6.4. The cardholder shall not be liable if the damage results from non-authorized use of the card during an online payment after the blockage has been ordered pursuant to Clause 7 unless the cardholder has acted with fraudulent intent.

7. Blockage of the authentication method 3D Secure

7.1. Automatic blockage
For security reasons, the authentication method 3D Secure will be blocked by the bank after the personal security features have been entered incorrectly five times in a row. As long as blockage is active, the cardholder cannot give any payment orders using the authentication method 3D Secure.

7.2. Blockage by the cardholder
The cardholder can perform blockage of 3D Secure due to the five-time consecutive incorrect entry of the security features himself/herself or have it blocked at +43 (0)5 99 06-6220.

7.3. Blockage by the bank

7.3.1. The bank is entitled to block the authentication method 3D Secure for the cardholder in the event of objective security reasons justifying such or in the event of non-authorized or fraudulent use.

7.3.2. The bank will inform the cardholder of blockage of the authentication method 3D Secure and of the reasons for such blockage to the extent possible prior to, but, at the latest, immediately after blockage, to the extent that blockage notification or the reasons for the blockage do not violate a court or administrative-authority order and/or would be contrary to Austrian or community-law legal norms or objective security considerations.

7.4. Notification and deactivation of blockage

7.4.1. Before a blockage becomes permanent, the cardholder will receive a warning.

7.4.2. The bank will deactivate blockage pursuant to 7.3. as soon as the reasons for blockage are no longer existent. The bank will inform the cardholder immediately of blockage deactivation.

7.4.3 The cardholder can order deactivation of the blockage at +43 (0)5 99 06-6220.

8. Changes of the Special Terms and Conditions for participation in 3D Secure for rechargeable PayLife prepaid cards

8.1. Changes of the Special Terms and Conditions for participation in 3D Secure for rechargeable PayLife prepaid cards will be offered to the cardholder by the bank at minimum two months before the proposed date of their entry-into-force; in this process, the terms affected by the change offer and the proposed changes to these terms are displayed in a comparison attached to the change offer (referred to as "comparison" in the following). The change offer will be communicated to the cardholder. The cardholder's consent is deemed to have been granted if the bank does not receive any written objection or any electronically-declared objection in the manner agreed with the cardholder (e.g. per e-mail). In the change offer, the bank will inform the cardholder that his/her silence due to the omission of a written objection or an electronically- declared objection in the manner agreed with the cardholder shall be deemed as consent to the changes, and that the cardholder, in his/her capacity as consumer, is entitled to cancel the agreement on participation in 3D Secure as well as the prepaid-card agreement before the entry-into-force of the changes without notice and free-of-charge. Morever, the bank will publish the comparison as well as the complete version of the new terms on its website and send the complete version of the new terms to the cardholder upon the latter's request; also to this fact, the bank will draw attention in the change offer.

8.2. The cardholder may be notified of the proposed changes in any way agreed with him/her. As such form shall also be deemed the communication of the change offer including the comparison to the e-mail address announced to the bank by the cardholder.

8.3. Any changes of these terms shall be confined to objectively justified cases. The following shall be deemed as objective justifications:

(i) if the change is required due to a change of the legal provisions relevant for payment services as well as for the handling of payment services or due to provisions enacted by the Financial Market Authority, the European Banking Supervisors, the European Central Bank or the Austrian National Bank,

(ii) if the change is required due to the development of the case law relevant for payment services as well as for the handling of payment services,

(iii) if the change enhances the security of banking operation or the security of handling the business relationship with the cardholder via participation in 3D secure,

(iv) if the change is required for the implementation of technological developments or for the adaptation to new programs for the use of end devices,
(v) if the change is required due to a change in the legal provisions applicable for issuing orders and for submitting declarations concerning the participation in 3D Secure,
(vi) if the change is required due to a change in the legal provisions applicable for the banking transactions that the cardholder can handle via 3D Secure.

The introduction of fees or the changes of agreed fees by way of a change of the STC at hand shall be excluded.

9. Change of cardholder's e-mail address and mobile phone number

The cardholder undertakes to announce any change of his/her e-mail address and mobile phone number to the bank either in writing or per e-mail. This shall not affect the provision under Clause 16. of the GTC.

10. Security notes

10.1. As long as access to the authentication method 3D Secure is blocked, the card cannot be used for payment purposes at Internet merchants to the extent that they offer 3D Secure.
10.2. To prevent risks connected to gaining knowledge of the identification features (in particular of the 3D Secure password) the bank recommends changing them at regular intervals (e.g. each month).
10.3. If the cardholder should suspect that his/her identification features (in particular the 3D Secure password) have come to the attention of third parties, the bank recommends changing the identification features.
10.4. Cardholders are advised to secure access to the use of mobile data terminal devices. In the event of loss or theft of the mobile data terminal device the bank recommends contacting the mobile telephony provider for the purpose of SIM card blockage.
10.5. Please note that the use of passwords on shared computers and mobile data terminal devices (e.g. in an Internet café, in a hotel, at the workplace) enables unauthorized third parties to spy out passwords.
10.6. On the www.paylife.at website, the bank will make available further information on the secure systems as well as security advice under menu item "Service".

11. Duration of contract, cancellation and termination

11.1. The agreement on participation in 3D Secure is concluded for an indefinite period of time.
11.2. The cardholder is entitled to cancel the agreement at any time without having to state any reasons for such and without having to observe a notice period. After receipt of the cancellation, the bank will block access to the authentication method 3D Secure.
11.3. The bank is entitled to cancel the agreement at any time by observing a two-month notice period and without having to state any reasons for doing so.
11.4 The cardholder as well as the bank are entitled to cancel the agreement at any time and with immediate effect in the event of good cause.
11.5 The termination of the agreement shall not affect the prepaid-card agreement unless the cardholder/the bank simultaneously declare the termination of the latter.
11.6 The agreement shall automatically end upon the end of the prepaid-card agreement.

as of September 2019, version of March 2020