Bacstel-IP

Business Customer Agreement for the TrustAssured Service

These terms and conditions, the CERTIFICATE POLICIES and all other documents referred to herein set out the terms of agreement (the "Agreement") between you and AIB Group (UK) p.l.c. for the use of the TRUSTASSURED SERVICE. This Agreement will be concluded once we accept your application by countersigning your BUSINESS CUSTOMER APPLICATION FORM.

Please note that these terms are in addition to any terms that already relate to your dealing and account(s) held with us and/or other members of AIB Group (UK) p.l.c. and, in the event of any inconsistency between those terms and the terms of this Agreement specifically relating to the SERVICE, the terms of this Agreement will prevail.

Recitals

(i). Whereas the TrustAssured Service is an electronic commerce tool which permits a customer to confirm their identity, or to verify the identity of third parties, by means of digital signatures

(ii). Whereas the infrastructure of TrustAssured Service is owned by Identrust;

(iii). Whereas The Royal Bank of Scotland p.l.c. (RBS) is authorised by Identrust to provide processing services in relation to the TrustAssured Service;

(iv) Whereas RBS has entered into an agreement to make its processing services available to AIB Group (UK) p.l.c.;
.

(v) Whereas AIB Group (UK) p.l.c. wishes to offer the TrustAssured Service to its customers

Definitions

AIB Group (UK) p.l.c. has a common set of definitions that are used in this Agreement and the other documents referred to in this Agreement. A definition for words appearing in capitals in these documents can be found in Schedule A to this Agreement.

1. Permitted Use of the Service and Your Responsibilities

1.1. You and your AUTHORISED SECURITY CONTACT(S) may use the PERSONALISED SMART CARD(s), Smart Card reader(s), the SOFTWARE, HSM(s) and the SERVICE:

1.1.1. to sign electronically data and other communications to be sent to us and any RELYING CUSTOMER; and

1.1.2 to encrypt data and other communications to be sent to us and any RELYING CUSTOMER;

1.1.3 to encrypt data and other communications to be sent to us and any RELYING CUSTOMER;

1.1.4 to validate and authenticate digital signatures used to sign data and/or other communications received from us or SUBSCRIBING CUSTOMERs.

PROVIDED THAT such use is in the EUROPEAN UNION countries specified in Schedule A, the United States of America, or any other Jurisdictions that are also APPROVED by TrustAssured, and is otherwise strictly in accordance with the terms of this Agreement (including the CERTIFICATE POLICIES) and is solely for the purposes of your business. Personal use by you or your AUTHORISED SECURITY CONTACT(S) is strictly prohibited.

1.2. You and your AUTHORISED SECURITY CONTACT(s) shall promptly comply with such USER INSTRUCTIONS as we may issue from time to time. USER INSTRUCTIONS may be issued by phone, fax, e-mail or post.

1.3. You and your AUTHORISED SECURITY CONTACT(s) must not use your KEY PAIR(s) and CERTIFICATE(s), PERSONALISED SMART CARD(s), Smart Card reader(s), the SOFTWARE, HSM(s) or the SERVICE in connection with anything that:

1.3.1. is illegal, unlawful or otherwise prohibited under any applicable law;

1.3.2. involves any transaction for which you are not acting as a principal or as agent for a principal that has been disclosed to us in writing;

1.3.3. is abusive, indecent, menacing, obscene, offensive, defamatory, in breach of confidence; or

1.3.4. is in breach of any intellectual property rights or other third party rights.

1.4. You are responsible for the supply and maintenance of the computer system(s) required to enable you to receive and use the SERVICE, and for ensuring compliance with the minimum configuration requirements specified by us for the time being and from time to time. You are responsible for obtaining any extra HARDWARE and SOFTWARE needed to ensure that your computer systems (including HSMs) are, and continue to be, compatible with the SERVICE and for the cost thereof.

1.5. You acknowledge that you are familiar with, and agree to comply with, the policies and procedures established by us relating to the issuance, suspension, re-activation, expiration and revocation of

CERTIFICATE(s) issued to you and your AUTHORISED SECURITY CONTACT(s) that are detailed in the relevant CERTIFICATE POLICIES. Copies of the CERTIFICATE POLICIES are available on request.

1.6. You and your AUTHORISED SECURITY CONTACT(s) must only use HARDWARE and SOFTWARE, including HSMs, to access or otherwise use the SERVICE that complies with such specifications and requirements as IDENTRUST may require.

1.7. You acknowledge that the laws of some countries restrict the use, import or export of encryption HARDWARE and SOFTWARE. Where you and/or your AUTHORISED SECURITY CONTACT(S) take the SOFTWARE (or any computer on which it is installed), HSM(s) or PERSONALISED SMART CARD(s) outside the United Kingdom you undertake to fully comply with local laws and regulations relating to their export and in particular you undertake to obtain any licence or approval that may be required
.

1.8. Before relying upon a digital signature generated by a SUBSCRIBING CUSTOMER, you or your AUTHORISED SECURITY CONTACT(S) must authenticate and validate the signature using the SERVICE.

2. Appointment and Revocation of AUTHORISED SECURITY CONTACTS

2.1. You may nominate two or more individuals to receive and utilise PERSONALISED SMART CARD(s) on your behalf in accordance with the following procedure:

2.1.1. your AUTHORISED SIGNATORY must complete, sign and return to us a BUSINESS CUSTOMER AUTHORISED SECURITY CONTACT Application Form which contains the details of the person(s) who you would like to become (an) AUTHORISED SECURITY CONTACT(S);

2.1.2. you must satisfy yourself as to the identity of each person who you would like to become an AUTHORISED SECURITY CONTACT by examining sufficient personal identification such as a passport, driving licence, or National Insurance card.

2.1.3. you must obtain the written consent of your AUTHORISED SECURITY CONTACT(S) to the processing of their personal information in accordance with clause 15.2.

2.2. You shall permit us or our authorised agents, on reasonable notice, to carry out an audit during normal working hours at your premises for the purpose of verifying compliance by you with clause 2.1.3 and you shall provide us or our authorised agents with access to such relevant DOCUMENTATION and equipment as may be necessary for this purpose.

2.3. We may refuse, for any reason, to issue a PERSONALISED SMART CARD to any person you have nominated to receive one.

2.4. If you wish to revoke or suspend an AUTHORISED SECURITY CONTACTS' CERTIFICATE (PERSONALISED SMART CARD), then your AUTHORISED SIGNATORY must sign and return to us, in accordance with the procedure set out in clause 10.3. below, a duly completed BUSINESS CUSTOMER AUTHORISED SECURITY CONTACT CERTIFICATE MANAGEMENT FORM.

2.5. If you wish to revoke or suspend an AUTHORISED SECURITY CONTACTS' CERTIFICATE (PERSONALISED SMART CARD), then your AUTHORISED SIGNATORY must sign and return to us, in accordance with the procedure set out in clause 10.3. below, a duly completed BUSINESS CUSTOMER AUTHORISED SECURITY CONTACT CERTIFICATE MANAGEMENT FORM.

3. Establishment and Revocation of TrustAssured Service Enabled Applications

3.1. In the event that you wish to use any SOFTWARE (other than the SOFTWARE in connection with the SERVICE) you must first seek our approval.

3.2. You will provide us with such information and access to such materials as we may require to enable us to assess your application for approval and to otherwise satisfy ourselves that the application you intend to operate will comply with such requirements as we and/or IDENTRUST may impose from time to time. If we approve your application we will issue you with your CERTIFICATE(s) and associated KEY PAIR(s) for usage on an HSM in respect of that application. The CERTIFICATE(s) and associated KEY PAIR(s) must only be used in respect of that application.

3.3. You are responsible for obtaining, maintaining and operating the HSM with which the application will be associated and for ensuring compliance with the minimum configuration requirements and all other technical and procedural requirements specified by us and/or IDENTRUST.

3.4. In the event that you wish to use or reproduce any of our, or 'IDENTRUST' trade marks, trade names, devices, logos or designs, you shall provide us with details of the name, mark, device, logo and/or design in question and the manner in which it is intended to be used. In the event that we approve such use, you shall be required to enter into a separate licence agreement.

3.5. We may, in our absolute discretion, refuse to approve any application under this clause 3 or subject use of it to such conditions, as we may deem appropriate.

3.6. If you wish to revoke or suspend a TRUSTASSURED SERVICE ENABLED APPLICATION'S CERTIFICATE your AUTHORISED SIGNATORY must complete and return a BUSINESS CUSTOMER-AUTHORISED SECURITY CONTACT CERTIFICATE MANAGEMENT FORM to the SERVICE OFFICE

3.7. Where you wish to upgrade, replace or implement any changes to any SOFTWARE approved by us under this clause 3, you must first seek our approval by submitting your request in writing to the SERVICE OFFICE. You must not make any such upgrades, replacements or changes unless and until approved by us.

4. Responsibility for Digital Transmissions

4.1. Subject to clause 4.2, you will be responsible for data and other communications signed digitally using KEY PAIR(s) and CERTIFICATEs issued by us to you or your AUTHORISED SECURITY CONTACT(s) where the Identity CERTIFICATE has been correctly confirmed through the SERVICE as not having expired, been suspended or revoked.

4.2. You will not be responsible under clause 4.1 in relation to digital signatures generated using Identity CERTIFICATEs issued by us to you or your AUTHORISED SECURITY CONTACT(s) where the request to validate the digital signature has been received by us after:

4.2.1 you have notified the SECURITY LINE in accordance with clause 5.4 that the security of your HSM or the PERSONALISED SMART CARD held by you or your AUTHORISED SECURITY CONTACT has been, or you believe it may have been lost, stolen, misused or compromised; or

4.2.2. you have requested the suspension or revocation of the applicable PERSONALISED SMART CARD or HSM (and related CERTIFICATEs) in accordance with the procedure set out in clause 10.3.

This clause 4.2 shall not apply where you or any of your AUTHORISED SECURITY CONTACTs have acted fraudulently or colluded with others who have done so.

5. Security

5.1. You are responsible for establishing and applying adequate security systems, controls and procedures in relation to:

5.1.1. the PERSONALISED SMART CARD(s), Smart Card reader(s), HSM(s) and SOFTWARE used by you and your AUTHORISED SECURITY CONTACT(s), to prevent their loss, disclosure to any other party, modification or use in breach of the terms of this Agreement;

5.1.2. monitoring all usage of the SERVICE by you and your AUTHORISED SECURITY CONTACT(s) including, without limitation, all use of PERSONALISED SMART CARDs and HSMs.

5.2. You and your AUTHORISED SECURITY CONTACT(s) must keep the PERSONALISED SMART CARD(s) and Smart Card reader(s) issued to you physically secure at all times and not leave them unattended. AUTHORISED SECURITY CONTACTs must not disclose their PIN(s) to anyone.

5.3. You must keep your HSM(s) physically secure at all times and comply with all security requirements imposed by us and/or Identrust in relation thereto at all time

5.4. You will provide immediate and accurate notice to the SECURITY LINE in accordance with the procedure set out in clause 10.3.1 of all relevant information relating to any actual or suspected loss, theft, misuse or compromise of the security of any HSM(s) or the PERSONALISED SMART CARD(s) held by you and/ or your AUTHORISED SECURITY CONTACT(s). In particular, if you suspect or become aware that a third party knows or has compromised the safekeeping of the PIN(s) or PRIVATE KEY(s) held by you (including within HSMs) or your AUTHORISED SECURITY CONTACT(s) you must notify the SECURITY LINE immediately.

6. Provision of the Service

We will provide the SERVICE to you under the terms and conditions of this Agreement until this Agreement is terminated.

7. Service Support

We will provide support for the SERVICE as described in Schedule C..

8. Charges

You agree to pay the applicable charges as set out in Schedule D, together with any taxes applicable, for use of the SERVICE.

9. Service Availability & Performance

The availability and performance of the SERVICE will be as defined in Schedule E.

10. Communication with AIB Group (UK) p.l.c.

10.1. This clause shall govern all communications from you to us relating to the SERVICE, including:

10.1.1. BUSINESS CUSTOMER AUTHORISED SECURITY CONTACT Application Form;

10.1.2. BUSINESS CUSTOMER AUTHORISED SECURITY CONTACT Certificate Management Form;

10.2. Subject to clause 10.3, all communications to be sent to us by you relating to the SERVICE can be by facsimile or by writing to the SERVICE OFFICE

10.3. The following types of communication must be sent to us in the following form:

10.3.1. a notice to be given under clause 2.5 must be given by fax to the SECURITY LINE followed by confirmation of the signed original to the SERVICE OFFICE;

10.3.2. the signed original BUSINESS CUSTOMER APPLICATION FORM must be submitted to the SERVICE OFFICE;

10.3.3. the signed original BUSINESS CUSTOMER AUTHO RISED SECURITY CONTACT Application Form must be submitted to the SERVICE OFFICE;

10.3.4. the BUSINESS CUSTOMER AUTHORISED SECURITY CONTACT Certificate Management Form must be submitted by fax followed by confirmation of the signed original to the SERVICE OFFICE;

10.4. We may act on any instruction that we receive relating to the SERVICE that has been signed by your AUTHORISED SIGNATORY, or otherwise reasonably appears to have been sent by you.

10.5. We may refuse to carry out an instruction if we reasonably believe that:

10.5.1. the instruction is invalid;

10.5.2. the instruction is invalid;

10.5.3. carrying out the instruction would result in a breach of the terms of this Agreement or of the rules of the IDENTRUST SCHEME. In the event that we do so, we shall endeavour tonotify you promptly thereafter.

11. Legal Effect

11.1. You agree that all data and other communications signed electronically using a KEY PAIR and CERTIFICATE(s) issued to you or one of your AUTHORISED SECURITY CONTACT(s) shall have the same legal effect, validity and enforcement as if the data and other communications had been in writing signed by you or that AUTHORISED SECURITY CONTACT (as the case may be).

11.2. You and your AUTHORISED SECURITY CONTACT(s) will not challenge the legal effect, validity or enforceability of data and other communications signed electronically using a KEY PAIR and CERTIFICATE issued to you or one of your AUTHORISED SECURITY CONTACT(s) solely on the basis that it is in digital rather than written form.

11.3. You and your AUTHORISED SECURITY CONTACT(s) shall not interfere with any procedures in relation to the logging or time-stamping carried out by the SOFTWARE or otherwise undertaken in connection with the SERVICE. Save in the case of manifest error or fraud, you acknowledge and agree that our records (including time stamps, logs and other material that is generated automatically) shall be deemed to be accurate unless the contrary is proven by you.

12. Call Recording

12.1. Telephone calls and e-mails may be monitored and/ or recorded by or on behalf of AIB Group (UK) p.l.c.:

12.1.1. for purposes of quality control and training;

12.1.2. to maintain and improve the SERVICE

12.1.3. for security reasons;

12.1.4. to establish the existence of facts in the event of a dispute or misunderstanding and to ascertain compliance with applicable regulatory or selfregulatory practices.

12.2. In the event that it is necessary to access a recording for these purposes, the access will be made under appropriate supervision.

13. .Accuracy of Information

13.1. You warrant the accuracy of all information supplied to us in relation to the SERVICE and, in particular, the BUSINESS CUSTOMER APPLICATION FORM and the other documents listed in clause 10.1. You will promptly notify us of any changes to the information described in this clause 13.1.

13.2. You will verify all information supplied to us that has been supplied by your AUTHORISED SECURITY CONTACT(s) in relation to the SERVICE.

13.3. You will ensure that on receipt of each PERSONALISED SMART CARD, each of your AUTHORISED SECURITY CONTACT(s) verifies that the information contained in the CERTIFICATE(s) on the PERSONALISED SMART CARD(s) is complete, accurate and up-to-date.

13.4. You will, on receipt of HSM(s), verify that the information contained in the CERTIFICATE(s) on the HSM(s) is complete, accurate and up-to-date.

13.5. You will promptly notify us when you would like to revoke or suspend the authorisation granted to an AUTHORISED SECURITY CONTACT or a TRUSTASSURED SERVICE ENABLED APPLICATION to utilise the SERVICE on your behalf.

14. Directory

14.1. You accept that your CERTIFICATE(s) may be published in our directory service that may be made available to other customers within the IDENTRUST SCHEME.

15. Transfer of Information

15.1. Subject to clause 15.2, we will use all reasonable endeavours to ensure that all information about you, your AUTHORISED SECURITY CONTACT(s) and your business received by or on behalf of us in connection with the SERVICE is kept confidential and is not disclosed to any third party. We are authorised to disclose information if that disclosure is:

15.1.1. made to the relevant authority where we are under a legal obligation to disclose the information; or

15.1.2. made in the course of the provision by us of the SERVICE in accordance with this Agreement and any USER INSTRUCTIONS given by us; or

15.1.3. made with your consent in accordance with clause 10 or 24.

15.1.3. made with your consent in accordance with clause 10 or 24.

15.2. Without prejudice to clause 2.1.3, you acknowledge that AIB Group (UK) p.l.c., RBS, other Participants, IDENTRUST and their employees and agents may and you hereby authorise each of them to, within the limits of applicable law, hold, transmit receive or otherwise process any data or information about, regarding or involving you and your AUTHORISED SECURITY CONTACT(s) among and between themselves and other third parties, both within the European Economic Area (EEA), and within countries outside the EEA:

15.2.1. to provide the SERVICE to you;

15.2.2. to resolve any dispute arising from the SERVICE; or

15.2.3. pursuant to applicable law.

15.3. You agree to treat (and to ensure that your AUTHORISED SECURITY CONTACT(s) treat) any information received through the SERVICE about other Customers as CONFIDENTIAL INFORMATION in accordance with clause 18.

16.Data Protection Notice
AIB Group (UK) plc Effective 25 May 2018

We respect your trust in us to use, store and share your information. In this notice, we explain how we collect personal information about you, how we use it and how you can interact with us about it.

We try to keep this notice as simple as possible but if you are unfamiliar with our terms, or want more detail on any of the information here, please see our

website's Frequently Asked Questions section or our contact details at

www.firsttrustbank.co.uk/data-protection or www.aibgb.co.uk/Data-protection. You can also ask for more details at your local branch.

16.1 Who we are

In this notice, 'we', 'us' and 'our' refers to AIB Group (UK) p.l.c. which includes First Trust Bank, Allied Irish Bank (GB) and Allied Irish Bank (GB) Savings Direct, and AIB Group which refers to Allied Irish Banks, p.l.c., its subsidiaries, affiliates and their respective parent and subsidiary companies. For more information about our group of companies, please visit

www.aibgroup.com.

We share your information within AIB Group to help us provide our services, comply with regulatory and legal requirements, and improve our products.

16.2 Data Protection Officer

Our Data Protection Officer oversees how we collect, use, share and protect your information to ensure your rights are fulfilled. You can contact our Data Protection Officer at UKDPO@aib.ie or by writing to them at: Data Protection Officer, AIB Group (UK) p.l.c., First Trust Centre, 92 Ann Street, Belfast, BT1 3HH.

16.3 How we collect information about you

We collect personal information from you, for example when you open an account; make a deposit; apply for products and services; use your credit or debit card; complete transactions; or look for advice. We also collect information through our website, apps, social media, discussion forums, market research and CCTV footage. We will sometimes record phone conversations and we will always let you know when we do this.

We may collect information to identify you through voice, facial or fingerprint (biometric data) recognition technology. We always ask for your consent to do this.

Our websites use 'cookie' technology. A cookie is a little piece of text that our server places on your device when you visit any of our websites or apps. They help us make the sites work better for you.

When you apply to us for products and services, and during the time you use these, we carry out information searches and verify your identity. We do this by sending and receiving information about you to and from third parties including credit reference agencies and fraud prevention agencies. We and these agencies may keep records of our searches whether or not the product or service goes ahead.

16.4 How we keep your information safe

We protect your information with security measures under the laws that apply and we meet international standards. We keep our computers, files and buildings secure.

When you contact us to ask about your information, we may ask you to identify yourself. This is to help protect your information

16.5 How long we keep your information

To meet our legal and regulatory obligations, we hold your information while you are a customer and for a period of time after that. We do not hold it for longer than necessary.

16.6 Meeting our legal and regulatory obligations

To use your information lawfully, we rely on one or more of the following legal bases:

- performance of a contract;
- legal obligation;
- protecting the vital interests of you or others;
- public interest;
- our legitimate interests; and
- your consent.

To meet our regulatory and legal obligations, we collect some of your personal information, verify it, keep it up to date through regular checks, and delete it once we no longer have to keep it. We may also gather information about you from third parties to help us meet our obligations. If you do not provide the information we need, or help us keep it up to date, we may not be able to provide you with our products and services.

16.7 Consent

Sometimes we need your consent to use your personal information. With direct marketing for example, we need your consent to make you aware of products and services which may be of interest to you. We may do this by phone, post, email, text or through other digital media.

You can decide how much direct marketing you want to accept when you apply for new products and services. If we ever contact you to get your feedback on ways to improve our products and services, you have the choice to opt out.

When we use sensitive personal information about you, such as medical or biometric data, we ask for your consent. Before you give your consent, we tell you what information we collect and what we use it for. You can remove your consent at any time by contacting us.

16.8 How we use your information

We use information about you to:

- provide relevant products and services;
- identify ways we can improve our products and services;
- maintain and monitor your products and services;
- protect both our interests;
- meet our legal and regulatory obligations; and
- decide and recommend how our products and services might be suitable for you.

To provide our products and services under the terms and conditions we agree between us, we need to collect and use personal information about you. If you do not provide this personal information, we may not be able to provide you with our products and services.

We analyse the information that we collect on you through your use of our products and services and on our social media, apps and websites. This helps us understand your financial behaviour, how we interact with you and our position in a market place. Examples of how we use this information includes helping protect you and others from financial crime, offering you products and services and personalising your experience.

We may report trends we see to third parties. These trend reports may include information about activity on devices, for example mobile phones, ATMs and self-service kiosks, or card spend in particular regions or industries. When we prepare these reports, we group customers' information and remove any names. We do not share information in these reports that can identify you as a customer, such as your name, or account details.

We sometimes use technology to help us make decisions automatically. For example, when you apply for a loan online. Before we make a decision, we automatically score the information you give us, any information we already hold about you, and any information we may get from other sources.

16.9 Your information and third parties

Sometimes we share your information with third parties.

For example to:

- provide products, services and information;
- analyse information;
- research your experiences dealing with us;
- collect debts;
- sell your debts;
- sell whole or part of our business;
- prevent financial crime;
- help trace, investigate and recover funds on your behalf;
- trace information; and
- protect both our interests.

in order to process your application we will supply your personal information to credit reference agencies (CRAs) and they will give us information about you, such as about your financial history.

We do this to assess creditworthiness and product suitability, check your identity, manage your account, trace and recover debts and prevent criminal activity.

We will also continue to exchange information about you with CRAs on an ongoing basis, including about your settled accounts and any debts not fully repaid on time. CRAs will share your information with other organisations. Your data will also be linked to the data of your spouse, any joint applicants or other financial associates.

The personal information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance or employment.

Further details of the CRA's and fraud prevention agencies, and how they process your information can be found at our websites.

We expect these third parties to have the same levels of information protection that we have.

We also have to share information with third parties to meet any applicable law, regulation or lawful request. When we believe we have been given false or misleading information, or we suspect criminal activity we must record this and tell law enforcement agencies, which may be either in or outside the UK.

16.10 International transfers of data

We may transfer your personal information outside of the European Economic Area (EEA) to help us provide your products and services. We expect the same standard of data protection is applied outside of the EEA to these transfers and the use of the information, to ensure your rights are protected.

16.11 Your personal information rights

You will find information about your rights, when they apply and our responsibility to you on our website's Frequently Asked Questions section.

You can exercise your rights by calling into a branch, using our social media channels, phoning or writing to us. Further information and our contact details are available on our websites at

www.firsttrustbank.co.uk/data-protection or www.aibgb.co.uk/Data-protection

Removing consent: You can change your mind wherever you give us your consent, such as for direct marketing, or using your sensitive information, such as medical or biometric data.

Restricting and objecting: You may have the right to restrict or object to us using your personal information or using automated decision making.

Deleting your information (your right to be forgotten). You may ask us to delete your personal information.

We can help you with:

Accessing your personal information: You can ask us for a copy of the personal information we hold. You can ask us about how we collect, share and use your personal information.

Updating and correcting your personal details.

Removing consent: You can change your mind wherever you give us your consent, such as for direct marketing, or using your sensitive information, such as medical or biometric data.

Restricting and objecting: You may have the right to restrict or object to us using your personal information or using automated decision making.

Deleting your information (your right to be forgotten). You may ask us to delete your personal information.

Moving your information (your right to Portability). Where possible we can share a digital copy of your information directly with you or another organisation.

When you contact us to ask about your information, we may ask you to identify yourself. This is to help protect your information.

We generally do not charge you when you contact us to ask about your information.

16.12 Making a complaint

If you have a complaint about the use of your personal information, please let a member of staff in your branch (or service outlet) know, giving them the opportunity to put things right as quickly as possible. If you wish to make a complaint you may do so in person, by telephone, in writing and by email. Please be assured that all complaints received will be fully investigated. You can register a complaint through our contact centre, our branches, our Website, by phone, by email or in person at your branch. We ask that you supply as much information as possible to help our staff resolve your complaint quickly.

You can also contact the Information Commissioner's Office at *www.ico.org.uk*

16.13 Updates to this notice

We will make changes to this notice from time to time, particularly when we change how we use your information, and change our technology and products.

You can always find an up-to-date version of this notice on our website at

www.firsttrustbank.co.uk/data-protection or www.aibgb.co.uk/Data-protection. You will also find a copy on display at your local branch, or you can ask us for a copy.

17. Ownership

Except as may be expressly provided for in this Agreement, you shall not obtain any rights, title or interest in the HARDWARE (including the KEY PAIR(s) and CERTIFICATEs contained therein), DOCUMENTATION, SOFTWARE, DIRECTORY ENTRIES and such other materials as may be provided to you and your of the SERVICE from time to time and you acknowledge that we and/or IDENTRUST and/or third parties own all such rights, titles and interests.

You are given no rights under this Agreement to use, copy or reproduce in any way any of AIB Group (UK) p.l.c.'s or RBS's trade marks, trade names, logos or designs.

You acknowledge that IDENTRUST is the sole and exclusive owner of all rights, title and interest in and to the IDENTRUST trade marks, trade names, logos or designs.

18. Confidentiality

18.1. Confidential Information' means all information of a confidential nature (including, without limitation, all information relating to the IDENTRUST SCHEME and all trade secrets, financial, operating, economic, technical, programming and other commercial know-how) and any copies or records thereof, whether presented orally or in writing, in any medium, directly or indirectly disclosed by us to you pursuant to or in connection with this Agreement, but excluding information which is:

18.1.1 in the public domain otherwise than in circumstances giving rise to a breach of the terms of this Agreement
;

18.1.2 already known to you at the time the information is disclosed by us;

18.1.3 subsequently received by you in good faith from a non-party to this Agreement who has the prior right to make such subsequent disclosure;

18.1.4 approved in writing for unrestricted release or unrestricted disclosure by us; or

18.1.5 developed independently by you other than from information disclosed by us or disclosed in breach of any of the obligations contained in this Agreement.

18.2. You and your AUTHORISED SECURITY CONTACT(s) must keep confidential all CONFIDENTIAL INFORMATION and not disclose it to any party or use it other than for the performance of this Agreement. You further agree that, without our prior express written consent, you shall never disclose, directly or indirectly, in whole or in part, alone or in conjunction with others, any CONFIDENTIAL INFORMATION to anyone other than to your employees and agents with a need to know such CONFIDENTIAL INFORMATION for purposes contemplated by this Agreement.

18.3. Notwithstanding clause 18.2, you shall be entitled to produce or disclose CONFIDENTIAL INFORMATION required by applicable law, regulation or court order, or any regulatory body or stock exchange, provided you have (if reasonably practicable) given us prior written notice of such request such that we have a reasonable opportunity to defend, limit or protect such production or disclosure.

18.4. Copies or reproductions of CONFIDENTIAL INFORMATION shall not be made except to the extent reasonably necessary and all copies made shall be our property.

18.5. You undertake immediately upon our written request in the event of a breach of this clause 18 by you or on termination of this Agreement whichever is the earlier either:

18.5.1. promptly to return all documents and other material on any medium whatsoever in your possession, custody or control that bear or incorporate any CONFIDENTIAL INFORMATION; or

18.5.2. promptly to destroy by shredding or incineration all documents and other materials on any medium whatsoever in your possession, custody or control that bear or incorporate any part of CONFIDENTIAL INFORMATION and to certify to us that this has been done.

19. Hardware and Software Licence

19.1. HARDWARE and SOFTWARE is licensed for use by you on the terms of this clause 19. Where the HARDWARE and/or SOFTWARE is subject to a licence granted by a THIRD PARTY PRODUCT PROVIDER, the provisions of clause 19.7 shall apply. The HARDWARE and/or the SOFTWARE shall be licensed to you on a non-exclusive, non-transferable basis for use by you and your AUTHORISED SECURITY CONTACT(s) only to enable you to obtain and use the SERVICE but not otherwise.

19.2. You must install and use such upgrades or replacements to the HARDWARE and SOFTWARE as may be made available from time to time as soon as possible after receipt of such upgrades or replacements. You will promptly comply with our USER INSTRUCTIONS regarding the materials being upgraded or replaced including returning them to us or destroying them if we so direct.

19.3. Save to the extent permitted by law, you must not and must not attempt to do any of the following or allow your AUTHORISED SECURITY CONTACT(s) or any third party todo so:

19.3.1. copy, publish, sell, rent, lease, de-compile, reverse engineer or modify the SOFTWARE or any part or parts thereof;

19.3.2. sell, rent, lease, reverse engineer, modify or tamper with any of the HARDWARE or any part or parts thereof.

19.4. All rights granted to you by this clause 19 shall terminate on termination of this Agreement.

19.5. You shall have no right to assign, sub-license or otherwise transfer any rights in any HARDWARE or SOFTWARE without our prior written consent.

19.6. IDENTRUST may in its own right enforce this clause 19

19.7. You acknowledge and agree that:

19.7.1. the licence granted by this clause 19 shall be subject to any licence granted to us by a THIRD PARTY PRODUCT PROVIDER of any of the HARDWARE and/or SOFTWARE;

19.7.2. you will comply with any additional terms imposed by the THIRD PARTY PRODUCT PROVIDER of any of the HARDWARE and/or SOFTWARE. Such additional terms will be notified to you either when the HARDWARE in question and/or SOFTWARE is/are provided to you or when you install and use them. If you refuse to accept any such terms you must return the HARDWARE and SOFTWARE to us and this Agreement will terminate on our receipt thereof and the provisions of clause 23 shall apply.

19.7.3. if any licence granted to us by a THIRD PARTY PRODUCT PROVIDER is terminated, the licence granted by this clause 19 will also terminate and you must stop using the HARDWARE and/or SOFTWARE (as the case may be) and destroy all copies of it or return them as instructed by us.

20. Recourse

20.1. When you or your AUTHORISED SECURITY CONTACT act as a SUBSCRIBING CUSTOMER:

20.1.1. You agree that your only recourse in connection with the SERVICE, including with respect to claims arising out of the negligence of any person, is to us and only to the extent provided for in this Agreement.

20.1.2. You expressly agree that you shall have no claim whatsoever against RBS in its capacity as a third party processor in relation to the provision of data certificate services

20.1.3. You agree that RBS shall be entitled to enforce, rely upon, and claim the benefit of, clauses 20.1.1 and 20.1.2.

20.1.4. You expressly recognise and agree that you have no recourse in this regard to Identrust or another Participant in connection with the SERVICE, but may have recourse or liability to the RELYING CUSTOMER under applicable law.

20.2. When you or your AUTHORISED SECURITY CONTACT act as a RELYING CUSTOMER:

20.2.1. You agree that you shall have no recourse of any kind against any party, except us or the SUBSCRIBING CUSTOMER, in connection with the SERVICE, including with respect to claims arising out of the negligence of any person.

20.2.2. You may have recourse to us to and only to the extent provided for in this Agreement and may have recourse or liability to the SUBSCRIBING CUSTOMER under applicable law.

21. Liability and Indemnity

21.1. We will take all reasonable care to prevent the release of viruses or other damaging code in provision of the SERVICE, related DOCUMENTATION or correspondence. However, we will not be liable for any damages that arise from this and you are advised to deploy your own antivirus mechanisms.

21.2. We shall not be liable to you either in contract, tort (including negligence) or otherwise for:

21.2.1. any loss or damage that you suffer as a result of your use of the SERVICE unless such loss or damage is caused directly by our negligence or by a breach of this Agreement by us;

21.2.2. any direct or indirect loss of profit, goodwill, business or anticipated savings nor for any indirect or consequential loss or damage resulting from your and/or your AUTHORISED SECURITY CONTACT(s) use of, or inability to use, the SERVICE, the HARDWARE or the SOFTWARE;

21.2.3. any losses resulting from third party services outside our reasonable control (including, but not limited to, telephone and browser services);

21.2.4. any loss caused by delay by us in performing or failure to perform our obligations under this Agreement if the delay or failure results from events or circumstances outside our control. Such delay or failure will not constitute a breach of this Agreement;

21.2.5. any loss suffered as a result of our refusal under clause 10.5.

21.3. Nothing in this Agreement shall limit either party's liability for death or personal injury resulting from its negligence or breach of this Agreement.

21.4. We expressly disclaim any warranty that data or communications sent or received through the SERVICE meet local legal requirements to effect a binding transaction or produce material that will be admissible as evidence in legal proceedings.

21.5. When you or your AUTHORISED SECURITY CONTACT act as a RELYING CUSTOMER, our liability to you for providing an incorrect IDENTITY VALIDATION shall be limited to £350 in respect of any single incorrect IDENTITY VALIDATION or series of related incorrect IDENTITY VALIDATIONs and is conditional on you informing us of any such claim within 14 days of the incorrect IDENTITY VALIDATION.

21.6. Our maximum aggregate liability to you howsoever arising from or in connection with this Agreement (whether for breach of contract, negligence, misrepresentaation or otherwise) shall not in any circumstances exceed the greater of £65,000 or the amount of charges paid by you to us in relation to the SERVICE over the one-year period preceding the event for which we are alleged to be liable.

21.7. You will indemnify us for any liability or loss incurred by us resulting from your or your AUTHORISED SECURITY CONTACT(s):

21.7.1. use of HARDWARE and/or SOFTWARE and any electronic messages or communications sent to persons or entities that are not RELYING CUSTOMERs of a Participant in the IDENTRUST SCHEME; or

21.7.2. failure to comply with the terms of this Agreement

.

22. Suspension of Service and Certificates

22.1. We reserve the right to suspend the SERVICE for repair, maintenance, and/or upgrade work. We will endeavour to give you such reasonable notice as circumstances permit but we do not guarantee that we will be able to do so in all cases. Notice may be given by facsimile, email, by phone or by post.

22.2. We reserve the right to suspend:

22.2.1. your access to the SERVICE where the SERVICE has not been used by you or any of your AUTHORISED SECURITY CONTACT(s); or

22.2.2. a given AUTHORISED SECURITY CONTACT's access to the SERVICE where the SERVICE has not been used by that AUTHORISED SECURITY CONTACT during the immediately preceding 90 day period.

22.3. Where access has been suspended under clause 22.2, we will reactivate your access to the SERVICE if you instruct us by re-submitting a request for reactivation in accordance with clause 10.

22.4. We may suspend and/or revoke CERTIFICATEs issued to you and/or your AUTHORISED SECURITY CONTACT(s) to protect our interests, RBS's interests, our CUSTOMERs' interests or IDENTRUST's interests, upon expiry of the SUSPENSION GRACE PERIOD, upon receipt of multiple suspension requests or upon termination of this Agreement, as described in the CERTIFICATE POLICIES.

23. Termination

23.1. Either party may terminate this Agreement by giving the other 30 days notice in accordance with clause 24.

23.2. We may terminate this Agreement forthwith on written notice if:

23.2.1. you are subject to an INSOLVENCY EVENT;

23.2.2. you or any of your AUTHORISED SECURITY CONTACTs persistently breach or commit a material breach of this Agreement which is not remedied within 30 days of a request to do so by us;

23.2.3. you or any of your AUTHORISED SECURITY CONTACTs commit, or attempt to commit, a fraud using the SERVICE or otherwise use the SERVICE in an illegal or unlawful way;

23.2.4. we cease to offer the SERVICE; or

23.2.5. you or your AUTHORISED SECURITY CONTACTs' use of the SERVICE is likely to bring us or the SERVICE into disrepute;

23.2.6 it is reasonably necessary to protect us and/or you.

23.3. Upon termination of this Agreement by either party:

23.3.1. provision of the SERVICE shall cease;

23.3.2. you and your AUTHORISED SECURITY CONTACT(s) must de-install the HARDWARE and SOFTWARE from your computer systems and, at our option, immediately destroy in accordance with our instructions or return promptly via secure courier to us at your cost, all KEY PAIRs, CERTIFICATEs, HARDWARE and SOFTWARE (including the media on which the SOFTWARE was originally provided along with any copies made by you or on your behalf and any copies of the KEY PAIRs and CERTIFICATEs held by you or on your behalf);

23.3.3. you must immediately pay to us any outstanding charges due under the SERVICE.

23.4. This agreement will continue until terminated in accordance with this clause 23.

24. Notice

24.1. Notices served by you under this Agreement must be made in writing to the SERVICE OFFICE and be signed by your AUTHORISED SIGNATORY(s).

24.2. Notices to be served by us under this Agreement shall be given to the contacts specified on the BUSINESS CUSTOMER APPLICATION FORM to the addresses set out therein. You may change your AUTHORISED SECURITY CONTACTS (or any of their details) at anytime by notice in writing, which change shall take effect upon approval thereof by us. Unless otherwise specified in this Agreement, notices shall be sent by post or fax followed by confirmation of the signed original to the SERVICE OFFICE.

25. Transfer of Rights

25.1. You are not entitled to assign, sub-licence or otherwise transfer any of your rights under this Agreement.

25.2. We expressly disclaim any warranty that data or communications sent or received through the SERVICE meet local legal requirements to effect a binding transaction or produce material that will be admissible as evidence in legal proceedings.

26. Sub-contractors

26.1. You may sub-contract any of your obligations under this Agreement without our consent.

26.2. If you do use such sub-contractors, such use shall be without prejudice to your obligations under this Agreement and you shall be responsible for all acts and defaults of the sub-contractor.

26.3. You must procure that sub-contractors shall be subject to provisions identical in all material respects to clauses 18, 19 and 23.

27. Dispute Resolution

27.1. Any dispute solely between you and us, arising out of or in connection with the SERVICE, not otherwise provided for in this clause 27, shall be settled in accordance with our DISPUTE RESOLUTION PROCEDURE for the TRUSTASSURED SERVICE.

27.2. You agree that any dispute between you and any Participant (other than us) and/or IDENTRUST or any dispute with us that involves related claims by or against other Participants and/or IDENTRUST arising out of or in connection with the SERVICE or the IDENTRUST SCHEME shall be finally settled pursuant to the IDENTRUST DISPUTE RESOLUTION PROCEDUREs. You expressly consent to being joined as a party to any DISPUTE RESOLUTION in respect of such disputes and in accordance with the IDENTRUST DISPUTE RESOLUTION PROCEDURE(s).

28. Waiver and Whole Agreement

28.1. No act, omission or delay by us shall be a waiver of our rights or remedies under this Agreement unless otherwise agreed in writing by us.

28.2. This Agreement and the documents referred to herein constitute the whole agreement between AIB Group (UK) p.l.c. and you relating to the SERVICE and supersede any previous agreement between the parties in relation to the SERVICE. All terms which may be implied by law into this Agreement are hereby excluded.

28.3. You acknowledge that you have not been induced to enter into this Agreement by any representation, warranty or undertaking not expressly incorporated into it. So far as permitted by law and except in the case of fraud, you agree and acknowledge that your only rights and remedies in relation to any representation, warranty or undertaking made or given in connection with this Agreement shall be for breach of the terms of this Agreement.

28.4. If any term of this Agreement is held to be invalid, the remaining terms of this Agreement shall continue to be valid to the fullest extent permitted by law.

29. Third Party Rights

29.1. Except as provided in clause 19 and clause 20.1.3 , nonparties may not enforce this Agreement by virtue of the Contracts (Rights of Third Parties) Act 1999

29.2. No consent will be required from any non-parties to vary the terms of this Agreement.

30. Variation

30.1. We reserve the right to vary the terms of this Agreement or the other documents referred to herein at any time provided that we give you at least two months' prior notice before such changes take effect.

30.2. We reserve the right to change any aspect of the SERVICE. We will give you reasonable notice of such changes.

31. Applicable Law

Applicable Law

The terms and conditions of this Agreement will be construed in accordance with English law and will be subject to the nonexclusive jurisdiction of the English courts.

SCHEDULE A

Definition of Terms

In this Agreement the following terminology shall have the following meanings.
'TrustAssured Service' or '**Service**' means the service to be provided under the terms of this Agreement as described in Schedule B.

'TrustAssured Service Enabled Application' means a computer service / application that has been constructed to make use of the Service.

'Approved' means that the jurisdiction has been assessed by the TrustAssured PAA for suitability and if found to be an acceptable jurisdiction that the necessary application form (Business Customer Application Form) has then been provided to the Customer to allow them to request provision of the Service.

'Authorised Security Contact' means any person issued with a Personalised Smart Card at your request pursuant to the procedures set out in clause 2. **'Authorised Signatory'** means that (or those) individual(s) that is (are) authorised by your Business, and accepted by AIB Group (UK) p.l.c., from time to time, to sign the Business Customer Application Form and to authorise instructions to AIB Group (UK) p.l.c.

'Business' means a limited company; partnership; sole trader; club; society; charity; trust or other unincorporated body.
'Business Customer Application Form' means the application form for the Service that forms part of the Agreement between you and AIB Group (UK) p.l.c.

'Business Customer Authorised Security Contact Application Form' means the application form to be used for the nomination of Authorised Security Contact(s) of the Service that forms part of the Agreement between you and AIB Group (UK) p.l.c.

'Business Customer Authorised Security Contact Certificate Management Form' means the form to be used for the deletion, suspension and re-activation of Authorised Security Contact(s) of the Service that forms part of the Agreement between you and AIB Group (UK) p.l.c.

'Certificate' means an X.509 v.3 compliant digitally signed data structure that immutably binds a Public Key to information uniquely identifying the possessor of the Private Key corresponding to such Public Key and that is issued by a Participant to a Customer under the Identrust Scheme.

'Certificate Policies' means the documents issued by AIB Group (UK) p.l.c. that set out the broad policy constraints that are imposed by RBS certification authority concerning the operational use of Certificates issued within its infrastructure. Policy documents are issued for Identity and Utility Certificates
'Confidential Information' shall have the meaning given in clause 18.

'Customer' means an entity that has entered into an agreement with a Participant governing the provision of services under the Identrust Scheme to the entity by that Participant.

'Directory Entries' means a database of Certificates and other information relating to users of the Service.

'Dispute Resolution' means a dispute to be conducted in accordance with one of the Dispute Resolution Procedures.
'Dispute Resolution Procedure for the TrustAssured Service' means the procedure contained in a document of that name as provided to you and as varied by us from time to time in accordance with this Agreement.

'Dispute Resolution Procedures' means the Identrust Dispute Resolution Procedures and the Dispute Resolution Procedure for the TrustAssured Service.

'Documentation' means material published by us, and/or Identrust, and/or third parties that describes the functionality or instructions on using the Service.

'European Union' includes only the following Countries: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Slovenia, Spain, Sweden, United Kingdom.

'Hardware' means any equipment provided to you by us or on our behalf for use of the Service including, without limitation, Personalised Smart Card(s), Smart Card reader(s), Hardware Security Module (HSM) and/or other hardware token(s), including any updates issued to you.

'Hardware Security Module' or **'HSM'** means an electronic device attached to a computer system that is used to securely hold the cryptographic keys.

'Helpdesk' means the Customer Helpdesk maintained by us to provide information and assistance to you in relation to the Service.

Contact details:

Bacs Customer Service,
First Trust Centre
92 Ann Street
Belfast
BT1 3HH

Tel: (01604) 235515
Email: bacssupport@aib.ie

'Identity Certificate' means a Certificate that is issued by an Issuing Participant to a Subscribing Customer under the Identrust Scheme to enable the Subscribing Customer to create digital signatures.

'Identity Validation' means the process whereby we validate and authenticate a digital signature for you as part of the Service. 'Identrust' means Identrust, LLC, a Delaware limited liability company.

'Identrust Dispute Resolution Procedures' means the process set forth in the Identrust Dispute Resolution Procedures document [IL-DRP] as varied from time to time for resolving a dispute arising from the Identrust Scheme.

'Identrust Scheme' means the infrastructure and scheme operated by Identrust for the provision of digital signature and identity validation services to Customers.

'Insolvency Event' means:

a) you at any time cease or suspend the payment of your debts or be or be deemed unable to pay your debts; or

(b) any step, application or proceeding is taken by you or against you, for your dissolution, winding up or bankruptcy or the appointment of a receiver, administrative receiver, administrator or similar officer to you or over all or any part of your assets or undertaking;

(c) where you are a partnership, such partnership is dissolved or joins or amalgamates with any other partnership;

(d) you commence negotiations with any of your creditors with a view to the general readjustment or rescheduling of your indebtedness, make a proposal for a voluntary arrangement or enter into an arrangement for the benefit of any of your creditors.

(e) you suspend or cease or threaten to suspend or cease all or a substantial part of your operations; or if any event occurs which, under the applicable law of any jurisdiction, has an analogous or equivalent effect to any of the events mentioned above.

'Issuing Participant' means, with respect to a Certificate, the Participant that issued that Certificate.

'Key Pair' means, with respect to any party in the Identrust Scheme, its Private Key and corresponding Public Key.

'Personalised Smart Card' or **'Smart Card'** means a card containing a computer chip that meets the specifications and standards specified by Identrust.

'PIN' (Personal Identity Number) means the eight (8) character random alpha/numeric code that must be entered in order to use your Personalised Smart Card.

'Public Key' means the key of an entity's asymmetric key pair that can be made public.

'Private Key' means one half of a cryptographic Key Pair (kept secret by the holder) as drawn from the class of asymmetric key cryptographic functions used in the Identrust Scheme that a Customer may apply to electronic data for identification purposes to generate a digital signature.

'Relationship Manager' means the individual identified on the Business Customer Application Form or their replacement from time to time.

'Relying Customer' means a Customer that requests from its Relying Participant confirmation of the status of a Certificate included in a digital transmission as a valid Certificate.

'Relying Participant' means the entity that provides services under the Identrust Scheme to a Relying Customer and that has entered into a Customer Agreement with that Relying Customer.

'Security Line' means the telephone line maintained by us to receive reports of security incidents, or suspected incidents, concerning the Service
Tel: (01604) 235515,

'Service' or **'the TrustAssured Service'** means the service to be provided under the terms of this Agreement as described in Schedule B.

'SERVICE OFFICE' means office maintained by us to which Customer application details and notices relating to the Agreement are to be addressed.

Contact details:

Bacs Customer Service,
First Trust Centre
92 Ann Street
Belfast
BT1 3HH

Tel: (01604) 235515
Email: bacssupport@aib.ie

'Service Owner' means AIB Group (UK) p.l.c.

'Subscribing Customer' means a Customer that obtains a Certificate from an Issuing Participant for use in connection with the Identrust Scheme.

'Software' means the software provided, or otherwise made available, to you by or on behalf of AIB Group (UK) p.l.c. from time to time for use in connection with the Service.

'Suspension Grace Period' means the period of time during which a Certificate can remain suspended, after which it is automatically revoked.

'We', 'our', 'us' means AIB Group (UK) p.l.c. 'Third Party Product Provider' means an external organisation that has developed and/or supplied Hardware and/or Software.

'User Instructions' means any guidance, advice, notification, letter or other communication from us to you that defines or otherwise explains how to use the Service or any part(s) of it.

'you', 'your' means the Business which has entered into this Agreement with AIB Group (UK) p.l.c. for the provision of the Service.

SCHEDULE B

The TrustAssured Service
Description of Service

The SERVICE consists of the provision of facilities and equipment to allow you to use digital signatures to confirm your identity in communications with us and third parties and the verification of the identity of parties sending communications including their digital signatures to you.

SCHEDULE C

The TrustAssured Service
Support Services

Under the terms and conditions of this Agreement, we will provide to you at the fees specified in Schedule D the following support services:

- Access to a telephone HELPDESK and SECURITY LINE between the hours of 09.00 and 17.00 Monday to Friday excluding English Bank and Public Holidays to:
- Receive general advice and guidance relating to usage of the SERVICE, completion of forms and any other aspects of the SERVICE.
- Receive technical support and guidance relating to the HARDWARE and SOFTWARE.•

- Report instances, or believed instances, of security

breaches relating to your PERSONALISED SMART CARD, PIN, HSM (if applicable) and PRIVATE KEYs.

- Request CERTIFICATE issuance, suspension, reactivation and revocation concerning your AUTHORISED OPERATORs and HSMs (if applicable).

- Provision of HARDWARE and SOFTWARE upgrades as determined and distributed by us from time to time.

- Provision of replacement HARDWARE and SOFTWARE (media) where the original becomes faulty or is lost / stolen and is correctly reported to us as a security compromise.

- Provision of new PERSONALISED SMART CARDs following CERTIFICATE renewal.

- Provision of configuration and operational changes as determined and distributed by us from time to time in the form of USER INSTRUCTIONS. We shall not be obliged to provide support in respect of:

- improper installation, use, operation or neglect of the HARDWARE or SOFTWARE;

- use of the HARDWARE or SOFTWARE for purposes for which it was not designed;

- any repair, alteration or modification of the HARDWARE or SOFTWARE (in whole or in part) by any person other than us or our agent, without our prior written consent or in breach of the terms of this Agreement;

- where applicable, your failure to install within a reasonable time any new release of HARDWARE or SOFTWARE issued to you by us;

- your use of a computer system other than as specified in USER INSTRUCTIONS issued by us;

- any unforeseeable impact on the existing applications on your computer system;

- any SOFTWARE or HARDWARE supplied by a third party, unless agreed by us in writing;

- failure to comply with USER INSTRUCTIONS, CERTIFICATE POLICIES or this Agreement;

- the introduction of any virus or other malicious code. If we agree to undertake additional support (which is not included in the support services described above), you will be advised of any costs payable before the additional support is provided.

SCHEDULE D

The TrustAssured Service
Charges Schedule

Please contact your RELATIONSHIP MANAGER or the SERVICE OFFICE for a current copy of our 'Business Banking - Charges Explained' brochure.

SCHEDULE E

The TrustAssured Service
Service Availability and Performance

The SERVICE will be made available to you 24 hours per day, 365 days per year, subject to the terms of this Agreement. Note that end to end performance throughout the SERVICE

cannot be guaranteed as it is formed from a number of services which are outside our control, e.g. Internet communication services, SUBSCRIBING CUSTOMER computer system, RELYING CUSTOMER application/service, Issuing and RELYING PARTICIPANTs' services (as appropriate).

If you need this brochure in Braille, in large print or on audio, ring 0345 600 5204† or ask your relationship manager. Customers with hearing difficulties can use our Text Relay Service by dialling 18001 0345 600 5204†.

† Calls may be recorded. Call charges may vary - refer to your service provider.
Call into any business centre | Phone 0345 600 5204† | www.aibgb.co.uk

Information correct as at May 2018