PRIVACY SHIELD NOTICE

Fidelity National Information Services, Inc. ("**FIS**") created this Privacy Shield Notice ("**Notice**") to help you learn about how we handle Personal Data transferred to FIS in the United States from the European Union ("**EU**") and the United Kingdom ("UK") in reliance on the Privacy Shield. This Privacy Shield Notice supplements the FIS Privacy Policy. Unless otherwise defined in this Notice, the capitalized terms used in this Privacy Shield Notice have the same meaning as in the FIS Privacy Policy. FIS protects all Personal Data we receive from the EU and the UK respectively. However, this Privacy Shield Notice applies only to Personal Data FIS receives from the EU and the UK respectively that is not otherwise covered by an alternative mechanism, such as Standard Model Contract Clauses.

FIS is subject to the jurisdictions of the U.S. Federal Financial Institutions Examinations Council (FFIEC), Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corp. (FDIC), Federal Reserve Bank (FRB), Security and Exchange Commission (SEC), Office of the Controller of the Currency (OCC), Office of Foreign Assets Control (OFAC) and the Federal Trade Commission (FTC), as well as other regulatory authorities around the world.

This Notice applies to certain wholly owned direct and indirect subsidiaries of FIS ("**Privacy Shield Companies**"):

Fidelity Information Services LLC;
FIS Financial Systems LLC;
WildCard Systems, Inc.;
eFunds Corporation; and
FIS AvantGard LLC.

Those named Privacy Shield Companies of FIS have subscribed to and adhere to the US-EU Privacy Shield program ("**Privacy Shield**") including the adoption and implementation of the Privacy Shield Privacy Principles (collectively, the "**Principles**") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU and the UK to the United States in reliance on Privacy Shield. FIS has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

FIS acquires Personal Data from the EU and the UK in a number of ways, including:

- EU or UK clients send credit and debit card application information to FIS for processing;
- EU or UK clients send account management related requests such as card status and information changes to FIS for processing;
- EU or UK clients or their underlying consumer customers send transaction-related data to FIS for processing;
- EU or UK clients send their underlying consumer customers' contact information to FIS, so FIS may contact such individuals to perform account management services;
- Individuals contact FIS to establish or manage their accounts with FIS EU or UK clients;
- FIS supports EU or UK clients by providing assistance and information to the EU or UK client's technical staff; and
- EU or UK clients may send personal data access requests to FIS for processing.

Information Received from the EEA

FIS provides a wide range of technology products for EU or UK clients in the banking and payment sectors such as payment processing, acquiring and authorizing card management and business process services, fraud prevention, and account management services. In order to provide these services, FIS receives information about the underlying consumer customers of these EU or UK clients including, but not limited to: names, office and personal telephone numbers, company and home addresses, card account numbers and transaction details, card website login credentials, and email addresses (collectively, "Personal Data").

Use of Personal Data

FIS uses Personal Data to perform its obligations under its EU and UK client agreements, including the following activities:

- Processing opening, change, or closing requests for underlying consumer customers on behalf of EU or UK clients;

- Processing opening, changing, or closing requests for cardholder accounts on behalf of EU or UK clients;
- Processing transaction information on behalf of EU or UK clients;
- Providing transaction screening services to EU or UK clients;
- Providing account management services to EU or UK clients;
- Providing EU or UK client support or implementation services for the above activities and for FIS software; and
- Processing Personal Data in accordance with the instructions of EU or UK clients.

Agents and Service Providers

FIS may periodically contract with other companies and individuals to perform functions or services described above, if we are permitted to do so under our agreements with EU and UK clients respectively. These agents and service providers may have access to Personal Data required to perform their functions, but the agents and service providers are restricted from using the Personal Data for purposes other than providing services for FIS. FIS requires its agents and service providers that have access to Personal Data received from the EU or the UK, as the case may be, to either: (i) subscribe to the Principles; or (ii) enter into a written agreement with FIS that requires the provision of comparable privacy protection as required by the Principles.

Onward Transfers to Third Parties

When transferring Personal Data to a third party acting as an agent, FIS transfers such information only for limited and specified purposes; confirms the agent is obligated to provide a comparable level of privacy protection as FIS; takes reasonable and appropriate steps to verify the agent effectively processes the Personal Data transferred in a manner consistent with FIS' obligations; upon notice, takes reasonable and appropriate steps to stop and remediate unauthorized processing; and, upon request, provides a summary or a representative copy of the relevant privacy provisions in its contract with that agent to designated authorities. FIS is potentially liable in cases of onward transfer to third parties of data of EU and UK data subjects, received pursuant to the EU-U.S. Privacy Shield.

Data Security

FIS uses reasonable physical, electronic, and administrative safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration, and destruction. FIS processing technologies and operations employ a wide range of security measures including: physical, electronic, and procedural safeguards; sophisticated security monitoring tools; documented security policies; use of encryption and/or private leased lines for transmissions of Personal Data to and from EU and UK clients; restricted access of personally identifiable information only to FIS employees that need to know the information; and periodic security audits by internal governance, compliance and audit groups and third party security experts.

Data Integrity

FIS takes reasonable steps to verify Personal Data we process is accurate, complete, reliable for its intended use, and current to the extent necessary for the purposes for which we use the Personal Data.

Data Rights including Access

Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. If you wish to exercise any of your data rights, such as the Right to Access, Deletion or Right to Data Portability under GDPR, you should submit your request to the EU or the UK client of FIS to whom you submitted the data. If you wish to review or correct your Personal Data that FIS maintains, you can send a written request to the address listed at the end of this Notice.

Choice

FIS will provide individuals with clear, conspicuous, and readily available opt-out mechanisms if FIS intends to use Personal Data for a purpose we know is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. If Sensitive Personal Data (i.e., Personal Data specifying medical or health conditions, racial or ethnic origin, etc.) is involved, FIS will obtain affirmative express consent (opt-in) from individuals, or confirmation that our client has done so, if such information will be used for a purpose FIS is aware of other than those for which it was originally collected or subsequently authorized by the individuals. In addition,

FIS will treat as sensitive any Personal Data received from a third party where the third party identifies and treats it as sensitive.

Principles Including Purpose Limitation

FIS will take appropriate steps to ensure Personal Data shall be processed in accordance with the Principles including:

- Lawfulness, fairness and transparency
- Purpose Limitation
- Data minimization
- Accuracy
- Storage Limitation
- Security
- Accountability.

Disclosure to Public Authorities

Certain governmental and regulatory entities may require FIS to share information about you to meet national security or law enforcement requirements. In these circumstances, only the specific information required by law, subpoena, or court order will be shared.

Privacy Shield Enforcement and Dispute Resolution

If you have any questions or concerns about this Notice or the Privacy Shield practices of the FIS Privacy Shield Companies named above, please write to us at the address listed below. FIS will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the Privacy Shield Principles.

Chief Privacy Officer
FIS
601 Riverside Avenue
Jacksonville, FL 32204, USA
E-mail: privacyoffice@fisglobal.com

Data Protection Officer
FIS
25 Canada Square, Canary Wharf
London E14 5LQ
United Kingdom
E-mail: privacyoffice@fisglobal.com

If after contacting the EU or UK client and FIS, an individual's complaint or dispute about Personal Data processing by an FIS Privacy Shield Company has not been resolved, the individual can contact the International Centre for Dispute Resolution of the American Arbitration Association at http://go.adr.org/privacyshield.html. FIS has engaged the ICDR/AAA as an independent dispute resolution provider to address unresolved Privacy Shield complaints. Under certain conditions, individuals may also invoke binding arbitration before the Privacy Shield Panel jointly created by the U.S. Department of Commerce and the European Commission.

.