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 Economic Area (collectively, the "**EEA**") 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 EEA. However, this Privacy Shield Notice applies only to Personal Data received from the EEA 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**"). More information about the Privacy Shield can be found at https://www.privacyshield.gov/.

FIS acquires Personal Data from the EEA in the following ways:

- EEA clients send credit and debit card application information to FIS for processing;
- EEA clients send account management related requests such as card status and information changes to FIS for processing;

- Transaction-related data is sent to FIS for processing, either directly from EEA clients or from their consumer customers;
- EEA clients send FIS contact information for their consumer customers, so FIS may contact such individuals to perform account management services;
- Individuals contact FIS to establish or manage their accounts with FIS EEA Clients;
- FIS supports EEA Clients by providing assistance to the EEA Client's technical staff; and
- EEA Clients send information access requests to FIS for processing.

Information Received from the EEA

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

Use of Personal Data

FIS uses Personal Data to perform its obligations under its EEA Client agreements, including the following activities:

- Processing opening, change or closing requests for individuals on behalf of the EEA Client;
- Processing opening, change or closing requests for cardholder accounts on behalf of the EEA Client;
- Processing transaction information on behalf of the EEA Client;
- Providing transaction screening services to EEA Clients;
- Providing account management services to EEA Clients; and
- Providing EEA Client support or implementation services for the above activities and for FIS software; and
- Processing Personal Data in accordance with the instructions of the EEA Client.

Agents and Service Providers

At times, FIS contracts with other companies and individuals to perform functions or services described above if we are permitted to do so under our agreements with EEA Clients. These agents and service providers may have access to Personal Data needed to perform their functions, but they 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 EEA to either: (i) subscribe to the Privacy Shield Principles; or, (ii) enter into a written agreement with FIS that requires the provision of comparable privacy protection as required by the relevant Privacy Shield 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. In cases of onward transfer to third parties of data of EU individuals, received pursuant to the EU-U.S. Privacy Shield, FIS is potentially liable**.**

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 EEA 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 reliable for its intended use, accurate, complete, and current to the extent necessary for the purposes for which we use the Personal Data.

Access to Personal Data

If you wish to review and correct the Personal Data FIS maintains about you, contact the EEA Client to whom you submitted the data and request access to your Personal Data from them directly. You may also ask to review and correct the Personal Data FIS maintains about you by sending a written request to the address listed at the end of this Notice.

Choice

In circumstances where FIS intends to use Personal Data for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals, those individuals will be provided with clear, conspicuous, and readily available mechanisms to opt-out of that use if they choose. 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 if such information is to be used for a purpose 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.

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, Florida 32204
E-mail: privacyoffice@fisglobal.com

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

.