FIRST DATA CORPORATION

SUMMARY: BINDING CORPORATE RULES FOR DATA PRIVACY AND PROTECTION

SUMMARY: BINDING CORPORATE RULES FOR DATA PRIVACY AND PROTECTION v 1.3	
Supersedes: v 1.2	
Summary Owner: **Corporate Privacy Office**	Summary Custodian: **David Tomlinson**
Distribution: **All employees**	Issued By: **John Atkins**
Approved by: John Atkins	Approved Date: March 3, 2014
	Effective Date: **March 3, 2014**
	Next Review Date: February 2015

Table of Contents

SUMMARY OF FIRST DATA CORPORATION'S BINDING CORPORATE RULES FOR DATA PRIVACY AND PROTECTION

Introduction

As a world leader in electronic commerce and payment services, First Data Corporation and its subsidiaries provide processing solutions that help businesses and consumers engage in financial transactions nearly anywhere in the world, any time of the day, with virtually anyone.

First Data operates offices in more than 36 countries globally. First Data employs approximately 24,500 employees to provide more than 60 billion payment transactions worldwide. First Data Corporation is the parent company of all First Data companies and is headquartered in the United States.

Since 2006, First Data has maintained Privacy Principles, designed to reflect First Data's continuing commitment to privacy and data protection compliance. The Privacy Principles, together with First Data's internal policies and other key documents, now constitute First Data's Binding Corporate Rules for Data Privacy and Protection ("**BCRs**").

The BCRs express the commitment of our employees, Executive Management and Board of Directors to data privacy to protecting all information relating to identified or identifiable natural individuals (known as "**Data Subjects**"). First Data processes certain information about Data Subjects while operating its business (known as "**Personal Data**"). First Data is committed to ensuring adequate protection for transfers of Personal Data between and among First Data companies. The BCRs set out First Data's overall approach to privacy and data protection and also emphasize the key role our employees play in protecting Personal Data.

Data protection laws give Data Subjects certain rights regarding how their Personal Data is handled. As a global company, First Data's use of Personal Data is subject to a variety of laws. In some countries, especially in Europe, Personal Data may not be transferred outside a country or region without demonstration of adequate data protection being in place prior to the transfer. Having and following BCRs is one method that First Data is using to comply with such laws and transfer restrictions.

First Data's BCRs are essentially a company-wide global privacy policy based on European data protection laws and standards and are enforceable by third parties. The BCRs contain rules and guidelines to be followed by all First Data employees and contractors. For ease and convenience, this document is a summary of key information in the BCRs. The full BCRs are available through the First Data Corporate Privacy Office and contain further detailed information about First Data's expectations and practices pertaining to Personal Data.

The Scope of the BCRs

The BCRs apply to all Personal Data used and collected by First Data entities wherever they are located. They are binding on all First Data entities that have signed a Binding Intra-Group BCR Membership Agreement and are referred to in this document as "**First Data,**" the "**First Data Entities,**" "**we**" or "**us**". As a result all First Data Entities are under a legal duty to comply with

the BCRs. An up-to-date list of these entities is available from the Corporate Privacy Office. However, the UK-based FDR Limited has overall responsibility for ensuring the compliance of the First Data Entities with the BCRs including remedying any breach of the BCRs.

Categories of Data Subjects and Purposes of Processing and Transfers

First Data processes and transfers Personal Data including Sensitive Personal Data relating to the following types of Data Subjects:

- Our clients and their customers in connection with the provision of services ("**Customer Information**");
- Individuals making payment transactions;
- Merchants accepting payments;
- First Data Employees, former employees, dependants and beneficiaries of employees, former employees, and prospective employees in connection with their working relationship or application for employment ("**Employment Data**");
- Other persons as appropriate to conduct its business such as suppliers, partners, contractors and contingent workers and prospective clients of First Data.
- "**Sensitive Personal Data**" in relation to the BCRs means any Personal Data about a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data about health or sex life, criminal record data, social security numbers and other national identifier numbers.

The processing and transfers undertaken by First Data relating to the types of Data Subjects discussed above include processing for the following business purposes:

- Employee Recruitment;
- Employee performance management and professional development;
- Payroll and administration of employee benefits;
- Research and development;
- Business development;
- Maintaining and building upon customer relationships;
- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;
- Maintaining the security of data collected and processed;
- Fulfilling a transaction initiated by or involving a Data Subject;
- Fulfilling a transaction with or for our clients;
- Providing the data to agents and contractors to assist us in our business, some of which may be located outside of the collection country;
- As authorized by the United States Fair Credit Reporting Act (15 U.S.C. §1681) or other applicable laws;
- For fraud prevention or investigation, or other risk management purposes;
- For identification and information verification purposes;

- For protecting First Data's legal rights or assets;
- Facilitating the acquisition or disposition of First Data businesses, including providing Personal Data to prospective purchasers;
- Enforcing our rights or the rights of other persons in a financial transaction;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process;
- On the written request of the Data Subject, where appropriate;
- Transferring certain data where necessary or required to other participants in a transaction processing chain, such as card associations and debit network operators and their members;
- In emergencies where the health or safety of a person is endangered;
- Other purposes required or permitted by law or regulation.

Nature of Data Transferred

First Data processes and transfers a broad range of Personal Data between First Data entities and to third parties. The types of Personal Data include:

- Employment Data: This includes data relating to health records, benefit information, staff development records, attendance records including any days off due to illness, salary remuneration and expenses information, expatriate information, equal opportunities management, grievance and disciplinary procedures, employee share equity holdings, employment termination information, names, addresses, date of birth, work location, employee performance, trade union membership and next of kin.
- Customer Information: This includes contact information of clients' employees, information relating to the client's account, clients' customers' contact details including name, address and telephone numbers and account information including other persons on the account and spend thresholds, details of clients' customers' spending and spending patterns and details of the merchants accepting payment transactions to the extent these are individuals.
- Other Personal Data: First Data also processes contact information of the employees of its suppliers and vendors and independent contractors including name, e-mail address, work location and telephone numbers and such other personal data as may be required in order for First Data to conduct business with such suppliers, and vendors and independent contractors.

A full description of the main types of Personal Data processed and transferred is available from First Data’s Corporate Privacy Office.

Applicable Law

We will handle Personal Data (including Sensitive Personal Data) in accordance with the BCRs and all applicable local data protection and privacy laws and regulations including, but not limited to, the European Union Data Protection Directive (Directive 95/46/EC), the Privacy in Electronic Communications Directive (Directive 2002/58/EC) (together the "**Directives**") and

the United States Gramm-Leach-Bliley Act (113 Stat. 1338) (the "**GLBA**"). The BCRs must be interpreted in accordance with the Directives, GLBA and all applicable data protection and privacy laws and regulations.

Where applicable data protection and privacy laws provide less protection than those granted by the BCRs, the BCRs will apply. Where applicable data protection and privacy laws provide a higher protection, they will take precedence over the BCRs.

As a general rule First Data does not assume any responsibility for compliance requirements that apply to its clients. Similarly, when First Data is acting as a data processor and not as a data controller, First Data is not responsible for interpreting, complying with, advising on, or ensuring its client complies with laws that apply to the client's business but do not apply to First Data's. In this circumstance, generally First Data acts in accordance with the client's instructions and the applicable contract provisions. Nothing in the Binding Corporate Rules or in this summary should be interpreted in any way to the contrary.

Data Protection Authority Cooperation

First Data will co-operate as reasonably required with any data protection authority that has approved the BCRs ("**Data Protection Authority**"). Any questions about First Data's compliance with applicable laws and regulations should be addressed to First Data's Chief Privacy Officer ("**Chief Privacy Officer**").

In addition, each Data Protection Authority may audit any First Data entity and advise First Data on matters related to the BCRs. First Data Entities will abide by formal and final decisions of the applicable Data Protection Authority related to the BCRs and where no further appeal may be pursued.

If a First Data Entity believes that a conflict with applicable laws prevents it from fulfilling its duties under the BCRs, the First Data Entity will notify the Local Privacy Officer and/or Chief Privacy Officer who will (in consultation with the First Data's General Counsel's Office or the relevant Data Protection Authority, where necessary) decide what, if any, action to take.

Changes to our BCRs and Transparency

First Data may change the BCRs, this summary or any relevant underlying documents from time to time. Current versions of the summary of the BCRs will be posted on First Data's public website and private intranet site. We will clearly indicate the effective date and the date of the latest revision to the BCRs. Any substantive changes will be reported to impacted First Data Entities and the relevant Data Protection Authorities at least annually after the change effective date.

Compliance and Dispute Resolution

If you have questions, concerns, or a complaint about First Data's compliance with the BCRs, you are encouraged to contact First Data's Chief Privacy Officer or his or her designee who will work with you to attempt to resolve the issue to your satisfaction. Contact information can be found at the end of this summary. The person investigating the issue will keep in regular contact

with you to ensure that you are kept informed of its review and resolution. We will strive to resolve it within five business days. Where that is not possible, for example due to the nature and complexity of the issue, we will keep in regular contact until the issue is resolved.

If the issue is not resolved to your satisfaction you can:

- raise the issue before the competent Data Protection Authority(ies); or
- bring the issue before either the courts of England and Wales or the courts of competent jurisdiction of the First Data entity making the transfer, at your option.

The rights contained in the BCRs are in addition to any other legal rights or remedies that you may otherwise have, including the right to compensation if appropriate.

Communication of First Data's Data BCRs

All First Data employees who handle Personal Data must comply with the BCRs and will receive training on the BCRs. First Data will also post a copy of the summary of the BCRs on its internal and public websites and will make physical copies permanently available at the Corporate Privacy Office. In addition, a copy will be sent to you on request.

First Data's Privacy Principles

All First Data Entities and employees will abide by the following principles when processing Personal Data.

1. We process Personal Data fairly and lawfully.

First Data processes Personal Data fairly and lawfully, in accordance with all applicable laws and regulations. Some First Data Entities may adopt their own privacy standards, policies and procedures based on the nature of their services or clients ("**Local Policies**"). The Local Policies will be consistent with and meet or exceed the requirements of the BCRs. Where there is a conflict between the Local Policies and the BCRs, the policy that offers the highest protection will govern.

2. We obtain Personal Data only for carrying out lawful business activities.

First Data collects, transfers, holds and processes Personal Data only for explicit and legitimate purposes as set out in the BCRs. First Data will not process Personal Data in ways incompatible with those purposes. Where we obtain Personal Data from third parties (including our clients) and publicly available sources, we always endeavor to use only reliable and reputable sources.

3. We limit our access to and use of Personal Data.

First Data limits access to Personal Data to those employees, contractors, agents and suppliers who reasonably need access to this data to fulfill their responsibilities and forbids employees from accessing or using this data for personal reasons or for any purposes other than fulfilling their First Data responsibilities. We require our contractors,

agents and suppliers to adopt a similar approach to Personal Data they access in connection with providing services to First Data.

First Data processes Personal Data in accordance with its written agreements or with instructions from our clients or business partners (as applicable), in compliance with applicable laws and our policies. In addition, our contracts and applicable laws govern our use of Personal Data received from vendors or other third parties.

4. We transfer Personal Data only for limited purposes.

First Data transfers Personal Data only when:

- all applicable legal requirements are met;
- the transfer is based on a clear business need;
- the receiving party has appropriate security;
- the receiving party, if a First Data Entity, complies with the BCRs for the transfer and subsequent processing of the Personal Data; and
- in the case of all transfers to third parties (including our clients) or to First Data entities not bound by the BCRs who are acting as a processor there is a written contract; (a) specifying that the receiving party will follow the exporting party's instructions; (b) setting out the rights and obligations of each party including provisions relating to security and confidentiality which they must follow; and (c) when transferring to a third party entity, ensuring that it has adequate security measures in place.

First Data does not disclose Personal Data except as set out in the BCRs, its policies or as required or otherwise permitted by contract or applicable law.

5. We use appropriate security safeguards.

First Data employs appropriate technical, organizational, administrative and physical security measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss or destruction. First Data regularly reviews and, as appropriate, enhances its security systems, policies and procedures to take into account emerging threats, as well as emerging technological safeguards and precautions. First Data will not transfer Personal Data to a country or territory which has inadequate data protection laws, unless adequate safeguards are in place.

When the processing of Personal Data is outsourced by First Data to a third party, First Data will select reliable third parties that have implemented appropriate security safeguards.

6. We provide transparency, choice and access as required by applicable data protection and privacy law.

First Data verifies Personal Data is kept up-to-date and current, accurate, adequate, relevant, and limited to the purposes for which it is collected and processed. We retain Personal Data only for the period of time that there is a business or legal need to do so.

First Data makes limited use of automated decision making in the processing of Personal Data. More information about our automated decision making practices are available upon request from the Corporate Privacy Office.

First Data will consider each reasonable request of a Data Subject for access to his or her own Personal Information and will, if technologically feasible, provide a copy of the Personal Data processed by First Data about that person unless there is a compelling reason not to. If a Data Subject submits a valid claim that the Personal Data First Data maintains about him or her is incorrect, we will work to rectify the inaccuracy.

When a Data Subject believes that First Data's processing of his or her Personal Data is likely to cause unwarranted substantial damage or distress, then the Data Subject may request in writing that First Data stops or does not begin processing that Personal Data. First Data will respond to such requests within 28 days.

7. We recognize a Data Subject's right to object to direct marketing by First Data.

First Data engages in direct marketing in accordance with applicable laws. First Data provides Data Subjects with the opportunity to opt out of marketing and honors those requests.

8. We recognize the importance of data privacy and hold ourselves accountable to our BCRs.

First Data, its Executive Management and its Board of Directors are committed to compliance with the BCRs. All First Data employees who handle Personal Data must understand and comply with the BCRs.

First Data employs a team of privacy officers who are responsible for facilitating data protection and data privacy compliance ("**Local Privacy Officers**"). These privacy officers share good privacy practices with employees within their region and conduct regular internal privacy assessments. Any First Data employee who materially violates any applicable data privacy or data protection laws or the BCRs may face disciplinary action up to and including dismissal.

Contact Information

Chief Privacy Officer and Corporate Privacy Office
First Data Corporation
6200 South Quebec Street
Greenwood Village, CO 80111
United States of America
Telephone Phone: +1 (303) 967-5186
Facsimile Number: +1 (303) 967-5185
E-mail Address: dataprivacyoffice@firstdata.com