AMENDMENT TO  
AGENCY AGREEMENT  
THIS AMENDMENT TO AGENCY AGREEMENT (this “Amendment”) is entered into as of the day of May, 2011 (the “Effective Date”) by and between XXXXXX STREET FUNDS, a businesstrust existing under the laws of the Commonwealth of Massachusetts, having its principal place of business at one Xxxxxxx Xxxxxx Xxxx, Xxxx, Xxxxxxxxxxxx 00000 (the “Trust”) and DST SYSTEMS, INC., a corporation existing under the laws of the State of Delaware, having its principal place of business at 000 Xxxx 00xx Xxxxxx, 0xx Xxxxx, Xxxxxx Xxxx, Xxxxxxxx 00000 (“DST”).  
WHEREAS, the Trust and DST entered into that certain Agency Agreement on the 13TH day of August, 2004 (the “Agreement”).  
WHEREAS, the Trust and DST wish to amend the terms of the Agreement as outlined below.  
NOW, THEREFORE, in consideration of the mutual promises, undertakings, covenants and conditions set forth herein, the Trust and DST agree as follows:  
1. Amendment to Agreement. With effect as of the Effective Date, the Agreement is hereby modified as follows:  
 (a)  
A new Section 19(K) is added as follows:  
(K) In connection with the enactment of the Red Flags Regulations (the “Regulations”) promulgated jointly by the Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC): Office of Thrift Supervision, Treasury (OTS); National Credit Union Administration (NCUA); and Federal Trade Commission (FTC or Commission) implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act:  
(1) DST shall assist the Trust to fulfill the Trusts’ responsibilities under certain provisions of the Regulations that focus on certain business processes that represent key activities of the transfer agent/service provider function, as set forth in the DST identity theft program (the “Identity Theft Program”), a current copy of which has hitherto been made available to Trust. These business processes are set forth in the Identity Theft Program. DST reserves the right to make changes thereto as experience suggests alternative and better ways to perform the affected function. DST shall provide Trust with written notice of any such changes thereto.  
(2) DST shall: (i) perform the procedures set forth in the Identity Theft Program, as amended by DST from time to time, which pertain to DST’s performance of those transfer agency services in accordance with the terms and conditions set forth in this Agreement, (ii) implement and maintain internal controls and procedures reasonably necessary to insure that DST’s employees act in accordance with the Identity Theft Program, and (iii) provide Trust with written notice of any material changes made to the Identity Theft Program.  
(3) Notwithstanding the foregoing, DST’s obligations shall be solely as are set forth in this Section 19(K) and in the Identity Theft Program and any obligations under the Regulations that DST has not agreed to perform under such Identity Theft Program or  
 130248v1 1   
under this Agreement shall remain the sole obligation of the Trust(s) or the Trust, as applicable.  
(4) With respect to the Identity Theft Program, DST will permit duly authorized governmental and self-regulatory examiners to make periodic inspections of its operations as such would involve Trust and the Trusts to obtain, inter alia, information and records relating to DST’s performance of its obligations under the Identity Theft Program and to inspect DST’s operations for purposes of determining DST’s compliance with the Identity Theft Program. Any costs imposed by such examiners in connection with such examination (other than fines or other penalties arising solely out of DST’s failure to fulfill its obligations under the Identity Theft Program) shall be paid by Trust.  
 (b)  
A new Section 22(D) is added as follows:  
Throughout the Term, DST shall comply with Exhibit D (DST Information Protection Program), which is made a part of this Agreement and applies to the Transfer Agency. The policies and procedures specified in Exhibit D (DST Information Protection Program) are subject to change at any time provided that the protections afforded thereby will not be diminished in comparison with those provided by DST to the Trust prior to the execution of this Agreement. DST will be reasonably available to meet with and provide reasonable assurances to the Trust concerning its data security procedures.  
2. Effect on Agreement. As of the Effective Date, this Amendment shall be effective to amend the Agreement and to the extent of any conflict between the Agreement and this Amendment, this Amendment supercedes and replaces the Agreement.  
3. Execution in Counterparts/Facsimile Transmission. This Amendment may be executed in separate counterparts, each of which will be deemed to be an original and all of which, collectively, will be deemed to constitute one and the same Amendment. This Amendment may also be signed by exchanging facsimile copies of this Amendment, duly executed, in which event the parties hereto will promptly thereafter exchange original counterpart signed copies hereof.  
4. Terminology. The words “include”, “includes” and “including” will be deemed to be followed by the phrase “without limitation”. The words “herein”, “hereof’, “hereunder” and similar terms will refer to this Amendment unless the context requires otherwise.  
5. Agreement in Full Force and Effect. Except as specifically modified by this Second Amendment, the terms and conditions of the Agreement shall remain in full force and effect, and the Agreement, as amended by this Amendment, and all of its terms, including, but not limited to any warranties and representations set forth therein, if any, are hereby ratified and confirmed by the Trust and DST as of the Effective Date.  
6. Capitalized Terms. All capitalized terms used but not defined in this Amendment will be deemed to be defined as set forth in the Agreement.  
7. Authorization. Each party hereby represents and warrants to the other that the person or entity signing this Amendment on behalf of such party is duly authorized to execute and deliver this Amendment and to legally bind the party on whose behalf this Amendment is signed to all of the terms, covenants and conditions contained in this Amendment.  
8. Governing Law. This Amendment shall be construed according to and governed by the laws of the State of Delaware.  
IN WITNESS WHEREOF, the parties have caused this Second Amendment to be executed by their duly authorized representatives as of the date first written above.  
 130248v1 0   
XXXXXX XXXXXX FUNDS  
By: /s/ Xxxxxxx Xxxxxxx  
Printed Name: Xxxxxxx Xxxxxxx  
Title: Vice President  
DST SYSTEMS, INC.  
By: /s/ Xxx X. Xxxxxxx  
Printed Name: Xxx X. Xxxxxxx  
Title: Vice President  
 3  
EXHIBIT D TO THE AGENCY AGREEMENT  
BETWEEN DST AND ADVISORS’ INNER CIRCLE FUND  
PAGE 1 OF 1  
DST Information Protection Program  
DST has a formal Information Protection Program (IPP) that was established and exists as a working roadmap for DST security. DST does Risk Assessments, Security Assessments, Security Awareness for the corporation as a whole, targeted training for specific applicable groups, and other security related activities. DST has a program and process pursuant to which DST reviews its technology and architecture and security requirements and needs.  
Integral to the function of the IPP are the Information Protection Committee (IPC) and the Information Protection Board (IPB). The IPC convenes periodically during the year and is responsible for 1) identifying, measuring and rating risks, 2) approving policies, standards, and practices, and 3) assessing and reporting progress towards compliance. The IPB convenes periodically during the year and is responsible for providing executive level oversight and guidance to the Information Protection Program.  
A component of the IPP is DST’s Policies, Control Standards, and Technology Baselines. DST’s Security Management Console (SMC) is an on-line system DST obtained from Xxxxxx Technologies that provides Security Policies, Control Standards, and Technical Baselines, oriented to the financial industry. The policies and standards incorporated in the SMC are designed to be consistent and evolve with IS027001, HIPAA, Data Protection Act of 1998, IS Forum Standards, FFIEC IS Booklet, and MAS to the extent DST deems them applicable to its business.  
DST has in place security log and activity monitoring, on a 24x7x365 basis. DST has an Intrusion Detection System (IDS) implemented to keep us informed on network activity. DST has an incident response process to deal with unexplainable logs and activities that are observed. This process is reviewed for validity and effectiveness for the purpose. DST uses third party security reviews to also provide the information to support DST’s security efforts.  
All of the foregoing policies and procedures are subject to regular review and modification without notice, it being agreed that (i) no change to the foregoing shall diminish the over-all level of security and protections afforded to Trust Data as maintained on TA2000 and the DST Facilities and (ii) DST hereby undertakes that it shall at all times have in place data security policies and standards that are reasonably designed to be consistent and evolve with IS027001, HIPAA, Data Protection Act of 1998, IS Forum Standards, FFIEC IS Booklet, and MAS to the extent DST reasonably deems them applicable to its business.  
 130248v1 4