LAW FIRM RETENTION AND BILLING POLICY

This Law Firm Retention and Billing Policy ("Policy") applies to all vendors providing legal services to TD Ameritrade Holding Corporation and its subsidiaries (collectively, "TD Ameritrade"). By agreeing to represent TD Ameritrade your firm agrees to comply with the terms of this Policy. Your firm's non-compliance with this Policy may result in TD Ameritrade's rejection of all, or part, of an invoice, or termination of its relationship with your firm.

I. RETENTION

Only a member of TD Ameritrade's Legal Department may retain you to work on a matter on behalf of TD Ameritrade, give you direction regarding a matter, or otherwise request that you perform billable services and/or incur expenses. You agree that if you are given direction or requested to perform billable services by someone at TD Ameritrade other than a member of the Legal Department, unless the matter requires immediate attention, you will contact the Legal Department before taking action on the direction or request.

If you require that TD Ameritrade execute a retainer or engagement letter, the terms of such retainer or engagement letter must not conflict with this Policy. In the event there is such a conflict, the terms of this Policy will govern.

At the time of retention, the Legal Department will have the matter(s) assigned to your firm through TD Ameritrade's chosen matter management and electronic billing provider, LexisNexis, a division of Reed Elsevier Inc. - CounselLink. You may be instructed to accept the matter assignment within CounselLink or the matter may be automatically accepted on behalf of your firm.

II. RATES AND EXPENSES

A. Hourly Rates

Hourly rates for all attorneys and staff who perform work for TD Ameritrade must be entered into CounselLink and approved by the Legal Department prior to performance of any billable services on any matter(s). Any proposed change in an hourly rate must be reviewed and approved in advance by the Legal Department. If a matter requires specific rates outside of what has been previously defined, a *Fee Structure Change Request* must be completed with the *Policy* contact.

TD Ameritrade is always interested in exploring alternative billing arrangements, such as caps, flat rates, or any other creative billing methods that result in economies for TD Ameritrade, while maintaining a fair return for your firm. If your firm would like to discuss these opportunities, please inform the Legal Department lawyer and the *Policy* contact.

B. Staffing

The Legal Department must approve in advance the seniority and number of lawyers (including partners and associates) and paralegals assigned to a matter. TD Ameritrade expects the minimum number of billers to be assigned to a matter in order to efficiently, as well as effectively, handle the matter. TD Ameritrade will not pay fees it believes to be the result of a duplication of effort.

C. Budget Estimates

Upon receipt of a matter, you must coordinate with the responsible Legal Department lawyer to provide an estimate of the scope of work, identification of major phases (when relevant) and projected costs (including for each phase, if relevant). As a matter progresses, you must timely inform the responsible Legal Department lawyer of any changes to the budget.

D. Coordination with Responsible Legal Department Lawyer

You are responsible to keep the Legal Department lawyer fully and currently informed about the status of pending matters and to consult with him/her regarding all significant decisions relating to the matter.

E. Use of Outside Third Parties

Use, selection and fee arrangements of experts, appraisers, consultants, special or local counsel, and any other third parties must be approved in advance by the Legal Department. In using outside local counsel, or any third party vendor, it is your responsibility to:

- provide a current copy of this *Policy*, with any attachment(s), to said counsel or vendor and
- Whenever possible, pay all third-party invoices and then submit those charges as disbursements on the firm's monthly invoice as an expense item, with supporting documentation/invoice attached using the 'Document Attachment' feature in CounselLink. Should an exception occur, contact Angeline Thompson to discuss handling.
    - See the instructions for attaching documents in Exhibit B.

Third Parties are not required to bill through CounselLink unless TD Ameritrade will be issuing payment to them directly.

F. Computer Legal Research

TD Ameritrade will not pay for computer legal research charges (*i.e.:* Lexis/Nexis, Westlaw, PACER, FastCase etc.) Any exceptions must be discussed in advance with, and approved by, the Legal Department lawyer.

G. Travel Expenses

TD Ameritrade will reimburse reasonable and necessary out-of-town travel expenses incurred in connection with the matter for which you have been retained, other than local travel. **Any local travel will not be reimbursed**. **Only Coach Class fares for air and train travel will be authorized; and if ground transportation is required, the cost for a midsize rental car will be authorized**. All travel reservations should take advantage of available discounts and special rates. Charges for attorney time during travel are not reimbursable if such time is used to perform services for a client other than TD Ameritrade. Extended travel time may require negotiation of a reduced hourly rate.

Copies of receipts for all travel expenses over $100.00 must be attached to all invoices using the Document Attachment feature in CounselLink and you must retain the original receipt for audit purposes. See the instructions for attaching documents in Exhibit B.

H. Disbursements

Disbursements will be reimbursed at the firm's cost; however, no profit, markups or administrative charges may be added. The following are **APPROVED** and **NON-APPROVED** disbursements by TD Ameritrade (subject to changes, as needed).

APPROVED	**NON-APPROVED***
Telephone Charges: ➢The actual cost of long distance telephone calls: **Provide the date of the call, city or telephone number called, and the actual cost of the call.**	Telephone Charges: ➢Charges for long distance telephone calls in excess of the actual cost of the call. ➢Local telephone expenses of any kind. ➢Cellular telephone charges.
FAX Charges: ➢The actual long distance charge for outgoing fax transmissions: **Provide the date of the fax transmission and the actual long distance charge.**	FAX Charges: ➢Charges for outgoing fax transmissions in excess of the actual long distance charge, or per-page charges. ➢Any incoming fax charges.

Computer Legal Research Services: ➢Record retrieval for documents filed in the specific matter(s) to which your firm is assigned.	Computer Legal Research Services: ➢ Research and record retrieval for any other matters, including but not limited to those used for general research or history.
Copying Charges: ➢Photocopying charges, Color or Greyscale, at no more than $.10 cents per page. ➢For large reproduction jobs, you should use a commercial copy center, if that will result in a savings to TD Ameritrade, and such disbursements will be reimbursed at actual cost. **Provide the number of copies and per copy cost, whether in-house or outside jobs.**	Copying Charges: ➢Photocopy expenses at more than $.10 cents per page. ➢Printing costs of any kind ➢Charges for scanning in electronic copies to disc or computer ➢Charges for converting or copying from one file type to another ➢Additional charges for Color Copies vs Greyscale Copies
Mail and Courier Charges: ➢Overnight mail and courier charges, but only when use of the service is absolutely necessary.	Mail and Courier Charges: ➢Mail costs.
Normal Law Firm Operating Costs or Overhead, including: ➢ Filing or proofreading charges. ➢ Any additional charges must be discussed in advance with, and approved by, the Legal Department lawyer.	Normal Law Firm Operating Costs or Overhead, including, but not limited to: ➢ Secretarial support or word processing charges, whether normal or temporary. ➢ Clerical charges. ➢ Overtime charges. ➢ Conference room charges. ➢ Time and costs for preparing, transmitting or resolving billing issues. ➢ Office supplies, including but not limited to; standard supplies, binding supplies, binder supplies, etc. ➢ Interest or other carrying costs or charges.

*If **NON-APPROVED** expenses are to be invoiced, they must be approved in advance by the Legal Department lawyer.

I. Litigation

In the interest of maximizing efficiency, controlling litigation costs, and facilitating the Legal Department's monitoring and supervision of lawsuits and arbitrations being handled by outside counsel, you must:

- Submit litigation budget to CounselLink, as outlined above, as soon as you have completed a preliminary review of a new matter;
- Review proposed staffing with the responsible Legal Department lawyer at the outset of the case, and confirm the staffing in writing;
- Maintain continuity of personnel;
- Stringently monitor and review bills for any unnecessary or excessive time or expenditures related to a matter;
- Consider and present to the responsible Legal Department lawyer cost-benefit alternatives including alternative methods of dispute resolution;
- Communicate and coordinate with the responsible Legal Department lawyer on all material aspects of the case, including strategy decisions;
- Provide on a monthly basis, written reports on the status of the matter and otherwise promptly communicate to the responsible Legal Department lawyer any significant developments in the case; and
- Maintain, in a retrievable manner, all relevant work-product.

III. INVOICE CONTENT AND PROCESS

A. Submission of Invoices

All invoices must be submitted to TD Ameritrade through CounselLink. Instructions on how to submit invoices to CounselLink are attached hereto as Exhibit A "Invoice Submission".

B. Billing Periods and Pre-Bill Estimates

Each invoice must contain a description of services performed and expenses incurred for one matter and for one calendar month only; an invoice that contains time billed for more than one matter, or more than one month, will be rejected.

Invoices for services performed and expenses incurred in one month must be submitted into CounselLink no later than the twenty-first (21st) day of the following month. Any invoices submitted for services performed or expenses incurred that are more than 180 days old for active matters are considered untimely and may not be paid, unless the reason for the delay in submitting the invoice was discussed and approved in advance with the responsible Legal Department lawyer. Invoices received more than 180 days after a matter has been closed are considered untimely and may not be paid.

Toward the end of each month, you will receive a notice requesting that the estimated unbilled legal fees and disbursements for each legal matter being handled by you for the current month (the "Pre-Bill Estimate") be entered into CounselLink. The request will contain a due date for submitting the Pre-Bill Estimate into CounselLink, which normally will be by close of business at the end of the month, or by the first or second day of the following month. It is essential that we receive your Pre-Bill Estimate by the due date for finance/accounting purposes. The Pre-Bill Estimate is used for financial accrual purposes only, and payment will not be made from a Pre-Bill Estimate.

C. Invoice Content

Invoice content will be entered into CounselLink as described in Exhibit A. If your firm wishes to include a supporting invoice your firm created, it may be attached as detailed in Exhibit B. **If there is a discrepancy between the supporting invoice and the information entered into CounselLink note that the information in CounselLink will take precedence.**

If a supporting invoice is provided, there must be a separate invoice submitted for each matter, showing the total amount due. Time for multiple matters, multiple months, or past due amounts should not be combined into one invoice.

The supporting invoice must contain at least the following:

- In the Header section:
  - Matter name (as defined in CounselLink)
  - TD Ameritrade's Matter Number (as defined in CounselLink)
  - Invoice date
  - Billing period covered by the invoice
  - Law Firm matter no. and Law Firm invoice no.
- In the Body section:
  - Detailed description of services rendered, including biller's initials, and time expended for each service. Time must be billed in units of 1/10 of an hour. Block billing will be rejected.
  - Listing of disbursements, including date and description of disbursement, and name of provider/vendor, if applicable.
    - **Copies of receipts for all expenses over $100.00, including third-party invoices, must be attached to all invoices using the Document Attachment feature in CounselLink and you must retain the original receipt for audit purposes.**
    - Instructions for attaching documents are detailed in Exhibit B.
- In the Summary section:
  - Full name, title and hourly rate of each billing individual (*i.e.:* Jonathan Smith - Partner - $400.00/hr)
  - Total number of hours billed by each billing individual during the current billing period

D. Prior Balances

Do not show or include any prior balances in any section, or in the total, of the current month's invoice. Invoice status may be viewed in CounselLink, including payment status. Inquires regarding payment status or unpaid invoices should be directed by email to the Legal Department lawyer and the *Policy* contact.

Invoices that do not contain all of the information detailed in Section III, or otherwise do not comply with this *Policy*, may be rejected and returned to your firm for resubmission in proper form.

IV. MISCELLANEOUS

A. Security and Integrity Measures

The nature of TD Ameritrade's business may result in your firm having access to personal, sensitive, confidential, or proprietary information. In light of the stringent requirements of securities and privacy laws, you must have and enforce (and must require that all subcontractors your firm uses for an engagement will have and enforce) necessary and appropriate security and integrity policies, procedures, programs, and other measures effective in preventing unauthorized use or disclosure of personal, sensitive, confidential, or proprietary information ("Security and Integrity Measures"). Such Security and Integrity Measures must be in accordance with the TD Ameritrade Vendor Information Security Policy ("VISP"), which is attached as Exhibit C and incorporated by reference into this Policy. The Legal Department may deliver additional instructions with respect to preserving the privacy and security of TD Ameritrade Data or Personal Data (both defined in the VISP).

Periodically during the engagement, TD Ameritrade may, but is not obligated to, perform or have a third party designee perform, security risk assessments of your firm as it relates to the receipt, maintenance, use or retention of TD Ameritrade Data. Your firm agrees to cooperate with TD Ameritrade in security risk assessments. The results of security risk assessments will be determined by TD Ameritrade in its sole discretion. Refusal to cooperate in a security risk assessment, or failure to comply with reasonable recommendations resulting from a security risk assessment, may result in termination of TD Ameritrade's relationship with your firm.

In the event any breach of security or confidentiality by your firm or its subcontractors implicates TD Ameritrade Data, TD Ameritrade will have sole control over the timing, content, and method of any required notification to an individual under any privacy or data breach law. TD Ameritrade may seek from your firm indemnification and reimbursement of TD Ameritrade's reasonable out-of-pocket costs in providing the notification and any fines or sanctions imposed on TD Ameritrade by any regulatory body having jurisdiction over them as a result of such breach.

Upon termination or completion of the engagement, your firm will delete or return any TD Ameritrade Data stored on the firm's systems or networks, and will destroy or return any copies of TD Ameritrade Data in its possession or control, as instructed by TD Ameritrade. Upon TD Ameritrade's request, the firm will provide to TD Ameritrade a written certification, executed by a duly authorized officer of the firm, confirming that all required return, destruction, or deletion of TD Ameritrade Data has occurred.

B. Auditing

TD Ameritrade reserves the right to audit, either directly or through a designee, all legal bills submitted by your firm, as well as corresponding legal files and contemporaneous time records, at any time while the file is active, or for a period of three years after the file is closed. TD Ameritrade's payment of any bill for legal fees or expenses will not constitute a waiver of its right to seek reimbursement for any overpayments disclosed by audit or otherwise.

C. Reassignment

TD Ameritrade retains the right to reassign matters to other counsel at any time. If such reassignment occurs, at TD Ameritrade's written request, you agree your firm will promptly transfer all files to new counsel at no cost to TD Ameritrade. A transfer of files will not constitute a waiver of any rights your firm or TD Ameritrade may have with respect to any claim for payment of fees or expenses.

D. Conflicts of Interest

You agree to advise the Legal Department at the earliest opportunity of any matter or relationships your firm has with other clients that could pose a conflict of interest – whether for a matter for which you are presently engaged or for other work which your firm could be asked to perform for TD Ameritrade in the future. We expect that you consider the potential for conflicts of interest broadly, and do not expect that you limit your consideration of this issue to the technical provisions of applicable Codes of Professional Responsibility. By agreeing to represent TD Ameritrade, you agree you will not hereafter accept representation of a client in a matter directly adverse to TD Ameritrade without the express written consent of TD Ameritrade, irrespective of whether such representation would technically be prohibited under applicable Codes of Professional Responsibility.

E. Contact

If you have any questions about the Policy, please contact Angeline Thompson, Legal Support Specialist, by phone at 402-574-6609 or by email at Angeline.Thompson@tdameritrade.com.

EXHIBIT A

INVOICE SUBMISSION

Invoice Submissions

To secure prompt and accurate payments to your firm, invoices in structured data format (LEDES) submitted via the web site www.counsellink.net are preferred. When necessary, we will accept invoices, in other formats, including e-mailing a .PDF or ASCII invoice or mailing a white paper invoice.

Submission of a Structured Data File to CounselLink

- Export the invoice to the LEDES (ASCII) structured data format
- Log into www.counsellink.net using your assigned login and password
- Click on the Upload Invoice link on the law firm home page
- Browse to the saved LEDES invoice, select it and click "Open"
- Complete any other necessary information on the Invoice Submission page and click "Submit File"

Creating an Invoice in CounselLink (U.S. currency only)

- Log into www.counsellink.net using the provided login and password
- Click on the Matter Search link on the law firm home page
- Search for the matter on which the invoice is to be submitted
- Select "Create Invoice" from the Action bar dropdown
- Enter information on the “Edit Invoice Screen” if applicable and click on Submit
- Enter fees and expenses from the invoice screen
- Submit invoice

Alternative Forms of Submission

- **Email**: A .PDF file or ASCII format copy of the invoice may be submitted via email to dept165@examen.com. Submit only ONE INVOICE PER .PDF file, although multiple .PDF files may be attached to a single email.

- **Paper**: An original copy of an invoice on white paper. If submitting paper invoices, a separate invoice must be submitted for each matter. When submitting invoices for multiple matters at one time, each invoice must begin on a new sheet of paper and must have a unique numerical identifier. Unique invoice numbers for individual matters may be created by adding a suffix to the invoice number created by your system (e.g., 12345-1, 12345-2, 12345-3, etc.)

  Paper invoices should be sent to [INSERT CLIENT NAME] c/o LexisNexis, a division of Reed Elsevier Inc. Attn: CounselLink Invoices, 1801 Varsity Drive, Raleigh, NC 27606

Invoice Returns

Invoices and the charges they reflect that in all respects conform to this Policy will be promptly processed for payment. Invoices or charges that do not conform to this Policy may be returned to your firm, in whole or in part, for correction. Invoices may also be returned for the following reasons:

- Firm has not acknowledged these guidelines
- Invoice is not in the proper format
- Invoice contains a math error
- Invoice contains block billed charges
- No invoice number
- Duplicate invoice number
- Invoice date is in the future
- Charge date is in the future
- Invoice is an exact duplicate of previous invoice
- Fee charges do not contain a date
- Fee charge does not contain date, timekeeper, units and rate
- Time increments not in tenths of an hour
- Unknown timekeeper
- No approved rate
- Expense charge has no description
- Unknown or incorrect LF Matter ID
- At Client's discretion

Block Billing on Invoices

Invoices should set forth in detail the related professional, the distinct tasks and activities performed by each professional, the time expended in tenths of an hour and fees charged for that work in separate time entries. Additionally, the task description must be sufficiently descriptive in order to identify the facility, location or office involved. Descriptions of blocks, batches of activities or tasks under one charge (i.e., "block-billing") are unacceptable. Invoices that contain any "block" billing entries will be returned.

For example, an invoice containing the following entry will be returned:

Hours	**Description**
1.5	Reviewed plaintiff's interrogatory responses; prepared letter to opposing counsel regarding settlement options; continue drafting motion for summary judgment.

If submitting a LEDES file, or emailing a PDF, an acceptable method to enter the time entry would be:

Hours	**Description**
1.5	Reviewed plaintiff's interrogatory responses (.3); prepared letter to opposing counsel regarding settlement options (.4); continue drafting motion for summary judgment (.8).

CounselLink Customer Support

CounselLink technical expertise is available to our outside counsel at no cost.

For technical support, please contact LexisNexis CounselLink's Customer Support Department at 800-600-2282, option 2, then 1. If outside the United States, please contact +1-919-378-2713.

EXHIBIT B

DOCUMENT ATTACHMENT

Law firms are able to attach case supporting documents such as pleadings, status reports and third-party invoices electronically to either an invoice or a matter. Outside counsel may be requested to upload specific documents to a matter or invoice. Documents will be permanently attached to the invoice or matter unless removed by the individual who attached them. Only the law firm and Client will be able to view the documents. Most document formats are accepted including PDF files.

PLEASE DO NOT USE DOCUMENT ATTACHMENT TO SUBMIT LAW FIRM INVOICES.

Attaching a document to an Invoice (e.g. expense receipts)

- Log in to http://www.counsellink.net
- From the Home page, click on either **Created** or **Scheduled** Invoices (dependent upon the status of your invoice)
- Click on the **CounselLink Invoice Number**
- To add or search for a document , click on the **Documents** link
- To add a document, click on the **Add Document** link
- Type in the document name as you want it to appear in CounselLink
- Browse your file directory for the document to add by clicking the **Browse** button
- Select the **Category** from the drop down
- Select "**Yes**" from the **Shared** drop down
- Select "**Public**" from the **Access Level** drop down
- Enter a free form description of the document in the **Description** box
- Enter a key word to assist in future searches in the **Key Word** box
- Click on **Save**

Attaching a document to a Matter (e.g. Initial Report, pleadings, summaries)

- Log in to http://www.counsellink.net
- From the Home page, click on **Matter Search**
- Enter the **Matter Search** criteria
- Click on the **Matter ID** or **Matter Title**
- Select **Documents** from the **Action** drop down
- Type in the document name as you want it to appear in CounselLink
- Browse your file directory for the document to add by clicking the **Browse** button
- Select the **Category** from the drop down
- Select "**Yes**" from the **Shared** drop down

- Select "**Public**" from the **Access Level** drop down
- Enter a free form description of the document in the **Description** box
- Enter a key word to assist in future searches in the **Key Word** box
- Click on **Save**

EXHIBIT C

VENDOR INFORMATION SECURITY POLICY

Updated: 07/31/2013

TD Ameritrade Holding Corporation and its Affiliates ("TD Ameritrade"), have established a comprehensive information security program to protect the confidentiality, integrity, and availability of information owned, controlled, or managed by TD Ameritrade ("TD Ameritrade Data", defined below). TD Ameritrade requires Vendors (hereinafter "Vendor") to materially comply with this Vendor Information Security Policy (the "Policy") to satisfy the minimum requirements of TD Ameritrade's information security program, unless otherwise agreed in advance in writing by TD Ameritrade with appropriate documentation of adequate compensating controls.

This is a policy of TD Ameritrade and may not be edited. Any variance from this policy for a Vendor must be separately agreed in writing executed by both Vendor and TD Ameritrade.

This policy applies to TD Ameritrade Data, including Personal Data.

1. GENERAL REQUIREMENTS

In all cases, TD Ameritrade requires that:

- All system security incidents involving this relationship shall be reported to TD Ameritrade's Security Event Center at the earliest possible time at eventcenter@tdameritrade.com and by phone at 800-229-6059. Notification must include enough detail so that TD Ameritrade can assess the scope and impact of such incidents and take additional action as necessary to safeguard the information.

- Vendor shall brief all Vendor Personnel (defined below) with access to the TD Ameritrade Data on the confidentiality and protection of TD Ameritrade Data (which shall include secure coding practices, if applicable).

- Access to TD Ameritrade Data for Vendor Personnel shall be on a "need-to-know" basis and restricted to allow only the minimum information required to fulfill contract requirements.

- Access privileges to TD Ameritrade Data by Vendor Personnel shall be assigned to individually identifiable accounts, and all activity conducted by these accounts must be auditable. Such access privileges shall be managed through the use of user ID's and passwords and shall not be shared or migrated to another individual. Additionally, biometrics, key tokens, or other security features that uniquely identify individuals may be used and are recommended.

- Vendor shall take commercially reasonable steps to prevent additional harm caused by security incidents involving TD Ameritrade Data and mitigation of harm shall always take priority over forensics.

- Vendor's protection of the TD Ameritrade Data shall be consistent with the terms of the agreements (the "Contract Documents") between TD Ameritrade and Vendor and all applicable laws and regulations, including Industry Standard Safeguards (defined below) to protect Vendor's systems used to store, transmit, and/or process TD Ameritrade Data.

- Vendor shall use commercially reasonable efforts to implement and maintain appropriate measures designed to:

    - Ensure the security and confidentiality of TD Ameritrade Data;
    - Protect against any foreseeable threats or hazards to the security or integrity of TD Ameritrade Data;
    - Protect against unauthorized access to or use of TD Ameritrade Data and Vendor's systems; and

- Upon request by TD Ameritrade, Vendor shall designate an individual who shall serve as TD Ameritrade's ongoing single point of contact for purposes of addressing issues with respect to the use and security of TD Ameritrade Data during the term and following the termination or expiration of the Contract Documents. Such individual will be accessible to TD Ameritrade and will cooperate with TD Ameritrade to address such issues.

2. SECURITY MEASURES

- Vendor shall maintain a written comprehensive information security program appropriate to the nature of the TD Ameritrade Data it handles, and shall provide documentation of their security policies and procedures to TD Ameritrade's Security Risk Management upon request. Upon request and with advance notice, Vendor shall allow TD Ameritrade reasonable access as necessary to review Vendor's system security environment to ensure all information accesses, security processes, and actual practices comply with this Policy.

- Vendor shall establish and maintain safeguards against the destruction, loss, alteration or misuse of TD Ameritrade Data in the possession of Vendor using safeguards that are no less rigorous than those used by Vendor for its own information of a similar nature.

- Vendor shall remediate security findings or risks in a manner reasonably acceptable to TD Ameritrade Security Risk Management. Upon request, Vendor shall provide reports of remediation progress to TD Ameritrade and allow access as necessary to inspect progress of such remediation. If such findings or risks cannot be remedied or mitigated in a mutually agreeable manner, TD Ameritrade may terminate its provision of the TD Ameritrade Data and request its return or destruction.

- Vendor shall communicate and coordinate any changes to Vendor's security infrastructure which directly affect the security of TD Ameritrade Data.

- If Vendor provides software (source or object code) that is operating on any TD Ameritrade network, TD Ameritrade shall be allowed periodic access to conduct security code scans (i.e., Fortify SCA, AppScan) or review the results of scans conducted by the Vendor as part of their application development process. Vendor shall coordinate application vulnerability remediation plans with TD Ameritrade Security Risk Management.

3. SPECIFIC SAFEGUARDS AND CONTROLS

Vendor shall maintain at least the following controls with respect to TD Ameritrade Data, consistent with Industry Standard Safeguards:

- Logical access controls to manage access to TD Ameritrade Data and system functionality on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, unique IDs and passwords, strong (i.e. two-factor) authentication for remote access systems, and elsewhere as appropriate, and promptly revoking or changing access in response to terminations or changes in job functions.

- Password controls to manage and control password complexity, expiration and usage for all user accounts associated with access to TD Ameritrade Data, whether directly or indirectly.

- Physical controls to protect information assets from environmental hazards and unauthorized access, and to manage and monitor movement of persons into and out of Vendor's facilities where TD Ameritrade Data is stored, processed, or transmitted.

- Operational procedures and controls to ensure technology and information systems are configured and maintained according to prescribed internal standards and consistent with Industry Standard Safeguards.

- Application security and software development controls designed to eliminate and minimize the introduction of security vulnerabilities in any software developed by Vendor for TD Ameritrade.

- Network security controls, including the use of firewalls, layered DMZs, and updated intrusion detection/prevention systems to help protect systems from intrusion and/or limit the scope or success of any attack or attempt at unauthorized access to Personal Data.

- Vulnerability management procedures and technologies to identify, assess, mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

- Encryption of Personal Data in accordance with the requirements as set forth in the Encryption section of this document and using algorithms and key lengths consistent with Industry Standard Safeguards to reasonably protect TD Ameritrade Data against unauthorized access, disclosure, or theft during transfer or storage, and as defined in this Agreement.

- Secure destruction of all Personal Data prior to sending any unencrypted hard disk, portable storage device, or backup media offsite for maintenance or disposal purposes.

- If a conflict exists between TD Ameritrade and Vendor's security protocols, TD Ameritrade and Vendor shall work to find a mutually agreeable solution.

4. VENDOR ACCESS TO TD AMERITRADE NETWORK AND SYSTEMS

To the extent that TD Ameritrade grants Vendor access to TD Ameritrade's computer network and/or telecommunications systems ("TD Ameritrade Network"), the following terms apply:

- Vendor's authorization to use the TD Ameritrade Network is specifically conditioned upon compliance with any technical requirements in the Contract Documents, including this Policy, and as may be provided to Vendor by TD Ameritrade in writing with respect to the access method. Vendor shall not cause, permit, or authorize any change, modification, enhancement, or additions to such technical requirements without the prior written consent of TD Ameritrade.

- TD Ameritrade reserves the right to monitor, inspect, or access Vendor's computer systems or other source devices when such devices are actively connected to or communicating with TD Ameritrade's Network or equipment, and intercept Vendor's communications traversing the TD Ameritrade Network or equipment at any time and without prior notice.

- TD Ameritrade may impose technical requirements or limitations upon Vendor's access and/or Vendor's computer systems for purposes of access to the TD Ameritrade Network, including requiring the assignment of permanent IP address(es) to Vendor's computer(s) for purposes of communication with the TD Ameritrade Network or equipment and requiring Vendor to provide to TD Ameritrade the names of Vendor personnel assigned to perform the services.

- Where Vendor personnel have access to the TD Ameritrade Network, Vendor shall notify TD Ameritrade as soon as is reasonably practicable of any changes in such Vendor personnel in order to permit TD Ameritrade to promptly revoke access of Vendor personnel to TD Ameritrade's systems and TD Ameritrade's Network. If TD Ameritrade grants Vendor access to the TD Ameritrade Network via Vendor's computer or other Vendor access device, Vendor agrees that prior to beginning such access it will have installed and activated up-to-date security products on such device, including but not limited to a host firewall and comprehensive anti-malware software (including virus and spyware protection). If Vendor becomes aware of any security issue (e.g. malware infection) with its access device when connected to the TD Ameritrade Network, Vendor shall promptly disconnect and notify TD Ameritrade.

5. TD AMERITRADE NETWORK ACCESS RESTRICTIONS

If granted access to the TD Ameritrade Network, Vendor may access the TD Ameritrade Network and associated applications solely for the purpose of providing designated services to TD Ameritrade. Vendor shall not use the TD Ameritrade Network, directly or indirectly, for any of the following purposes:

- to transmit to or receive from or communicate with networks, persons or entities other than TD Ameritrade and its officers and employees, except with prior written consent of TD Ameritrade (for example, one Vendor location may not use the TD Ameritrade Network to communicate directly or indirectly with other Vendor locations);

- to establish a peer to peer network connection between the Vendor's computer and any computer on the TD Ameritrade Network, the Internet, or Vendor's own network, without TD Ameritrade's prior written consent;

- for any unapproved use, including third party email or file transfer services (e.g., Gmail, Hotmail, Yahoo, AOL, etc.) or to conduct any kind of unapproved business or transaction other than with, or for the benefit of, TD Ameritrade;

- to access, copy or store any confidential, proprietary, private or Personal Data (defined below);

- to accomplish any illegal or unlawful purpose, or to do any activity which would violate any law, rule, regulation, ordinance, or decree of any governmental authority, or cause TD Ameritrade to be in violation of any such law, rule, regulation, ordinance, or decree, or which could subject TD Ameritrade to any sanction, civil or criminal;

- to access any data and/or network to which Vendor does not have prior authorization from TD Ameritrade;

- to upload, post, email, otherwise transmit, or post links to any material that contains malicious software, bots, viruses, spam, time bombs, trap doors, or any other computer code, files or programs or repetitive requests for information designed to intercept, transmit, or otherwise gain unauthorized access to information or to interrupt, destroy or limit the functionality of the TD Ameritrade Network, telecommunications equipment, or data, or any other party's network, or to diminish the quality of, interfere with the performance of, or impair the functionality of the TD Ameritrade Network or any other party's network.

6. DATA ENCRYPTION REQUIREMENTS

To the extent applicable, Vendor shall encrypt all Personal Data in accordance with the table below using current, industry-standard algorithms and key lengths to protect Personal Data against unauthorized access, disclosure, or theft during any physical or logical transfer or storage. To the extent Vendor cannot comply with the following requirements, Vendor shall provide notice to TD Ameritrade and the parties shall work together to develop procedures or schedules for encryption acceptable to TD Ameritrade.

Process	**Minimum Acceptable Encryption Method(s)**	**Example Solutions**
PersonalData transfer across any public network, including the Internet	IPSec, TLS or SSLv3 between hosts with minimum 128-bit symmetric key; 2048-bit asymmetric key	sFTP, OpenSSL, IPSec VPN tunnel
Transfer of Personal Data in email message body (i.e. non-bulk)	TLS transport layer encryption between email gateways of Vendor and TD Ameritrade	S/MIME, x.509, PGP

Transfer of Personal Data via email attachment (i.e. bulk transfer greater than 5 identities)	Encrypted attachment or point to point email encryption solution	S/MIME, x.509, PGP, WinZip (AES-256) w/ 15-character passphrase delivered using alternate communications method
Personal Data storage or transfer using portable devices (e.g. CD/DVD, laptop hard disks, PDA's, memory cards/sticks)	'Whole Disk' encryption or volume encryption using AES-256 with a minimum 15-character passphrase or two-factor authentication token required to decrypt	Safeboot (McAfee) Device Encryption, PGP Whole Disk, Mobile Armor, Microsoft BitLocker
Personal Data storage on archival media (i.e. backup tapes)	Personal Data is written to tape in encrypted form using Industry Standard algorithm, and/or full tape encryption with appropriate key management	Decru DataFort, NetBackup encryption, CommVault encryption, tape drive hardware encryption, PGP Archive containing Personal Data is written to backup tape
Personal Data stored on file servers or in application databases	File, container, or record level encryption using Industry Standard algorithm with appropriate access controls and key management	Microsoft EFS, SQL column encryption, PGP File or PGPDisk, TrueCrypt, WinZip encrypted archive

The encryption standards contained in the table above represent current minimum standards for Personal Data and may be modified by TD Ameritrade at any time when warranted to preserve the security of Personal Data. In the absence of prior express written permission from TD Ameritrade, Vendor shall not store Personal Data on any portable storage device unless no less than the minimum acceptable encryption method(s) above are in place.

7. SECURITY AUDITS

Vendor will provide TD Ameritrade, upon request, a summary report of any technical vulnerability assessments it has completed within the prior twelve (12) months, including a description of any significant (i.e. moderate or greater) risks identified and an overview of the remediation effort(s) undertaken to address such risks.

8. CHANGES

TD Ameritrade reserves the right to modify this policy as required.

9. DEFINITIONS

As used in this Vendor Information Security Policy:

"Affiliates" means any wholly owned subsidiary of TD Ameritrade or an entity which is controlled by TD Ameritrade of one of its wholly owned subsidiaries, or an entity under common control with TD Ameritrade.

"TD Ameritrade Data" means any data, whether in physical or electronic form including but not limited to documents, databases, records, intellectual property and confidential information (as defined elsewhere in the Contract Documents) created by or disclosed to Vendor in the course of providing services to TD Ameritrade that has been identified by TD Ameritrade as "Confidential" or "Restricted" or that a reasonable person would understand to be confidential, proprietary or trade secret information. TD Ameritrade Data includes Personal Data.

"Industry Standard Safeguards" means those safeguards widely accepted by information security professionals as necessary to reasonably protect data during storage, processing, and transmission; consistent with the sensitivity of and widely recognized threats to such data. Examples of Industry Standard Safeguards include, but are not limited to, those practices described in ISO/IEC 27002:2005, NIST 800-44, Microsoft Security Hardening Guides, OWASP Guide to Building Secure Web Applications, and the various Center for Internet Security Standards.

"Personal Data," a subset of TD Ameritrade Data, means any and all personal, medical, and/or financial data pertaining to an identifiable individual, living or deceased, as well as all types of data covered by applicable data privacy laws and/or regulations (including, but not limited to: Gramm-Leach-Bliley, Regulation S-P, the FACT Act, EU Data Protection Directive 95/46/EC, UK Data Protection Act of 1998, PIPEDA, HIPAA, federal and state data breach laws as enacted within the United States, and California AB 1298) that is created by or made available to Vendor and/or its affiliates by or on behalf of TD Ameritrade. Personal Data shall include any such data in any media or format, including both paper and electronic.

"Security Incident" means (a) the actual unauthorized access to or use of TD Ameritrade Data, or (b) the unauthorized disclosure, loss, theft or manipulation of unencrypted TD Ameritrade Data (or encrypted TD Ameritrade Data where unauthorized decryption has or is likely to occur) or other information under control of Vendor that has the potential to cause harm to TD Ameritrade's business, clients, employees, systems, or reputation.

"Vendor Personnel" are employees, agents and other persons including subcontractors and independent contractors providing services on Vendor's behalf.