

**Agenda – Regular Meeting
Tech Valley High School Operating Board
A Joint Venture of Capital Region BOCES and Questar III**

January 27, 2022 6:15 p.m. Tech Valley High School
SUNY Polytechnic Institute
College of Nanoscale Science and Engineering
246 Tricentennial Drive
Albany, New York 12203

District Superintendent: Ms. Anita Murphy, Capital Region BOCES
District Superintendent: Dr. Gladys Cruz, Questar III BOCES

1. Pledge of Allegiance
2. Approval of the Agenda and Waive 72 Hour Notice
3. Minutes
4. Recognition of Visitors
5. Privilege of the Floor
6. Review of the Financial Risk Assessment and Information Technology Reports for Tech Valley High School
7. Business Items
 - a. Board Policy -- Renumeration
 - b. Internal Claims Auditor Report
 - c. Treasurer's Report
 - d. Approval of Cash Management Master Agreement with T.D. Bank, N.A.
 - e. Acceptance of the External Audit Report for Tech Valley High School
8. Principal's Report
9. District Superintendents' Report
10. Board Discussions
11. Summary Actions
12. Adjournment

1. **Pledge of Allegiance**

2. **Approval of the Agenda**

RESOLVED: that the Tech Valley High School Operating Board approves the agenda as presented and add any items introduced by unanimous vote.

3. **Minutes**

RESOLVED: that the Tech Valley High School Operating Board approves Minutes from the November 18, 2021 Board Meeting. (copy attached)

4. **Recognition of Visitors**

5. **Privilege of the Floor**

6. **Review of the Financial Risk Assessment and Information Technology Reports for Tech Valley High School**

Ms. Alexa Schaefer, Internal Auditor, Questar III BOCES, will present the Financial Risk Assessment and Information Technology Reports pertaining to the Tech Valley High School.

RESOLVED: that the Tech Valley High School Operating Board accepts the Tech Valley High School Financial Risk Assessment and Information Technology Reports for 2020-2021. (copies attached)

7. **Business Items**

a. **Board Policy -- Renumeration**

RESOLVED: that the Tech Valley High School Operating Board approves renumeration of the following policy. This ensures consistent numbering of policies.

<u>Old Number</u>	<u>New Number</u>	<u>Policy</u>
8630	8330	Authorized use of BOCES-owned Materials and Equipment

The Tech Valley High School Board Policies can be found on the school's web page at the following address: <https://www.techvalleyhigh.org/operating-board/board-policies>.

b. **Internal Claims Auditor Report**

RESOLVED: that the Tech Valley High School Operating Board accepts the Internal Claims Auditor Report for November 1, 2021 through December 31, 2021. (copy attached)

c. **Treasurer's Report**

RESOLVED: that the Tech Valley High School Operating Board approves the Treasurer's Reports for the periods ending November 30, 2021 and December 31, 2021. (copies attached)

d. Approval of Cash Management Master Agreement with T.D. Bank, N.A.

RESOLVED: that the Tech Valley High School Operating Board hereby approves the cash management master agreement between the Tech Valley High School and **T.D. Bank, N.A.**, 54 Quaker Road, Queensbury, New York 12804. T.D. Bank, N.A. will provide banking services to the Tech Valley High School. The contract period is December 20, 2021 through December 19, 2024. This contract is based on RFP #21-019.York. (copy attached)

e. Acceptance of the External Audit Report for Tech Valley High School

RESOLVED: that the Tech Valley High School Operating Board accepts the corrected Tech Valley Regional Technology Institute Financial Report dated June 30, 2021. (copy attached)

8. Principal's Report

(copy attached)

9. District Superintendents' Report

10. Board Discussions

11. Summary Actions

12. Adjournment



REGULAR MEETING – November 18, 2021

A Regular Meeting of the Tech Valley Regional Technology Institute (Tech Valley High School), a joint venture of the Board of Cooperative Educational Services of Albany-Schoharie-Schenectady-Saratoga Counties, 900 Watervliet-Shaker Road, Albany, New York, and the Board of Cooperative Educational Services of Rensselaer-Columbia-Greene Counties, 10 Empire State Boulevard, Castleton, New York, was held on November 18, 2021 via Zoom, as directed in the Governor's Executive Order 202.1, due to the response to the COVID-19 Pandemic. The meeting was called to order at 6:35 p.m. by President Brooks.

PRESENT

John Bergeron
Edmund Brooks
John Hill
Lynne Lenhardt
John Phelan
Frank Zwack
Gladys Cruz, Dist. Supt.
Anita Murphy, Dist. Supt.
Gretchen Wukits,
Clerk of the Board

ABSENT

Lynn Clum
Nancy delPrado
Joseph Garland
Kevin Kutzscher

STAFF

Amy Hawrylchak

GUESTS

Wendy Ashley
Mike Buono
Harry Hadjioannou
Danielle Hemmid
Rafael Olazagasti
John Tafilowski
Shannon Tahoe
Anthony Taibi

Due to there not being a quorum at 6:25 p.m., it was decided that Mr. John Tafilowski, Cusack and Company, Certified Public Accountants LLC, would begin presenting the External Audit Report for TVHS for 2020-21 while the Board waited for the sixth Board member to arrive. Mr. Tafilowski began his presentation at 6:25 p.m.

REVIEW OF THE EXTERNAL AUDIT REPORT FOR TVHS

He extended his thanks to the Board and acknowledged Ms. Wendy Ashley, Director, Business Operations, and her staff for their assistance with preparations for the report. Mr. Harry Hadjioannou, Deputy Superintendent and Chief Innovation Officer, Questar III BOCES, raised a question about the amount of the *Proportionate Share of Net Pension Liability* under *Noncurrent Liabilities*. After discussion, it was determined that the amounts for the *Proportionate Share of Net Pension Liability* and the *Accrued Other Postemployment Benefits* had been transposed. Mr. Tafilowski stated the correction would be made, and copies of the corrected report would be submitted.

Dr. Bergeron arrived at 6:35 p.m. The meeting was called to order at 6:35 p.m. by President Brooks.

President Brooks led the Pledge of Allegiance.

**PLEDGE OF
ALLEGIANCE**

It was moved by Mrs. Lenhardt and seconded by Mr. Phelan to accept the agenda and to waive the 72-hour notice to add items to the agenda by unanimous resolution. The motion passed unanimously.

AGENDA

It was moved by Mr. Phelan and seconded by Mrs. Lenhardt to accept the September 23, 2021 Reorganization Meeting and the September 23, 2021 Board Meeting Minutes. The motion passed unanimously.

MINUTES

President Brooks formally acknowledged Mr. Tafilowski and Ms. Danielle Hemmid, Special Education Teacher, TVHS.

**RECOGNITION
OF VISITORS**

It was moved by Mrs. Lenhardt and seconded by Mr. Phelan to approve the following:

**REVIEW OF THE
EXTERNAL AUDIT
REPORT FOR TVHS**

RESOLVED: that the Tech Valley High School Operating Board accepts the Tech Valley Regional Technology Institute Financial Report dated June 30, 2021, contingent upon the correction of the transposed amounts of Proportionate Share of Net Pension Liability and Accrued Other Postemployment Benefits on pages 13, 30, and 32. The motion passed unanimously.

(continued)

It was moved by Dr. Bergeron and seconded by Mrs. Lenhardt to approve the following:

RESOLVED: that the Tech Valley High School Operating Board approves the fee of \$8,100 for independent audit services for the TVHS fiscal year ending June 30, 2022 in accordance with the agreement between Tech Valley High School and Cusack & Company, CPA's LLC. The motion passed unanimously.

**APPROVAL OF
AGREEMENT
BETWEEN TECH
VALLEY HIGH
SCHOOL AND
CUSACK &
COMPANY,
CPA'S LLC.**

It was moved by Dr. Bergeron and seconded by Mr. Zwack to ratify the following policy:

**BOARD
POLICIES –
SECOND AND
FIRST READINGS**

Policy Title

Number

Attendance

Policy No. 5100

The motion passed unanimously.

It was moved by Dr. Bergeron and seconded by Mr. Zwack to conduct a first reading of the following revised policy:

<u>Policy Title</u>	<u>Number</u>
Child Abuse Reporting Policy and Regulations	Policy No. 5300

In accordance with Policy #2040, Policy Development, which allows for the Board to waive a second reading and adopt a policy upon the first reading when an urgent need exists to do so or other circumstances so warrant, it was agreed to do so for Policy No. 5300, Child Abuse Reporting Policy and Regulations.

It was moved by Dr. Bergeron and seconded by Mr. Zwack to waive the second reading and to ratify the following policy:

<u>Policy Title</u>	<u>Number</u>
Child Abuse Reporting Policy and Regulations	Policy No. 5300

The motion passed unanimously.

It was moved by Dr. Bergeron and seconded by Mr. Zwack to approve the following:

**INTERNAL
CLAIMS
AUDITOR
REPORT**

RESOLVED: that the Tech Valley High School Operating Board accepts the Internal Claims Auditor Report for September 1, 2021 through October 31, 2021. The motion passed unanimously.

It was moved by Mr. Hill and seconded by Mrs. Lenhardt to approve the following:

**TREASURER'S
REPORTS**

RESOLVED: that the Tech Valley High School Operating Board approves the Treasurer's Reports for the periods ending September 30, 2021 and October 31, 2021. The motion passed unanimously.

It was moved by Mr. Zwack and seconded by Mr. Phelan to approve the following:

**ACCEPTANCE
OF DONATIONS**

RESOLVED: that the Tech Valley High School Operating Board hereby accepts the following in accordance with Capital Region BOCES Policy No. 2090:

A set of microfiber "Envirocloths" from Norwex.

Books in Chinese from the Confucius Institute (CI), University at Albany, State University of New York.

The motion passed unanimously.

Dr. Amy Hawrylchak, Principal and Chief Academic Officer, TVHS, provided an update on school operations and the ongoing implementation of COVID-19 protocols. She shared information on the development of a TVHS code of

**PRINCIPAL'S
REPORT**

values reflecting those of the NYSED and NTN Frameworks. Dr. Hawrylchak provided data on the change in Capital Region demographics and how that is reflected in the applicants and students of TVHS. In order to accommodate these changes, she said she was exploring translation services for parents of students.

Ms. Anita Murphy, District Superintendent, Capital Region BOCES, spoke about the opportunities afforded to students who attend TVHS and the attention of the Board of Regents to innovation at TVHS. Dr. Gladys Cruz, District Superintendent, Questar III BOCES provided an update on meeting with the TVHS staff and P-TECH grants.

**DISTRICT
SUPERINTENDENTS'
REPORT**

President Brooks welcomed Mr. Frank Zwack who rejoined the TVHS Operating Board.

**BOARD
DISCUSSIONS**

The following items are follow-up items for the next meeting.

**SUMMARY
ACTIONS**

- Corrected pages from External Audit Report

It was moved by Mrs. Lenhardt and seconded by Dr. Bergeron to adjourn the meeting at 7:25 p.m. The motion passed unanimously.

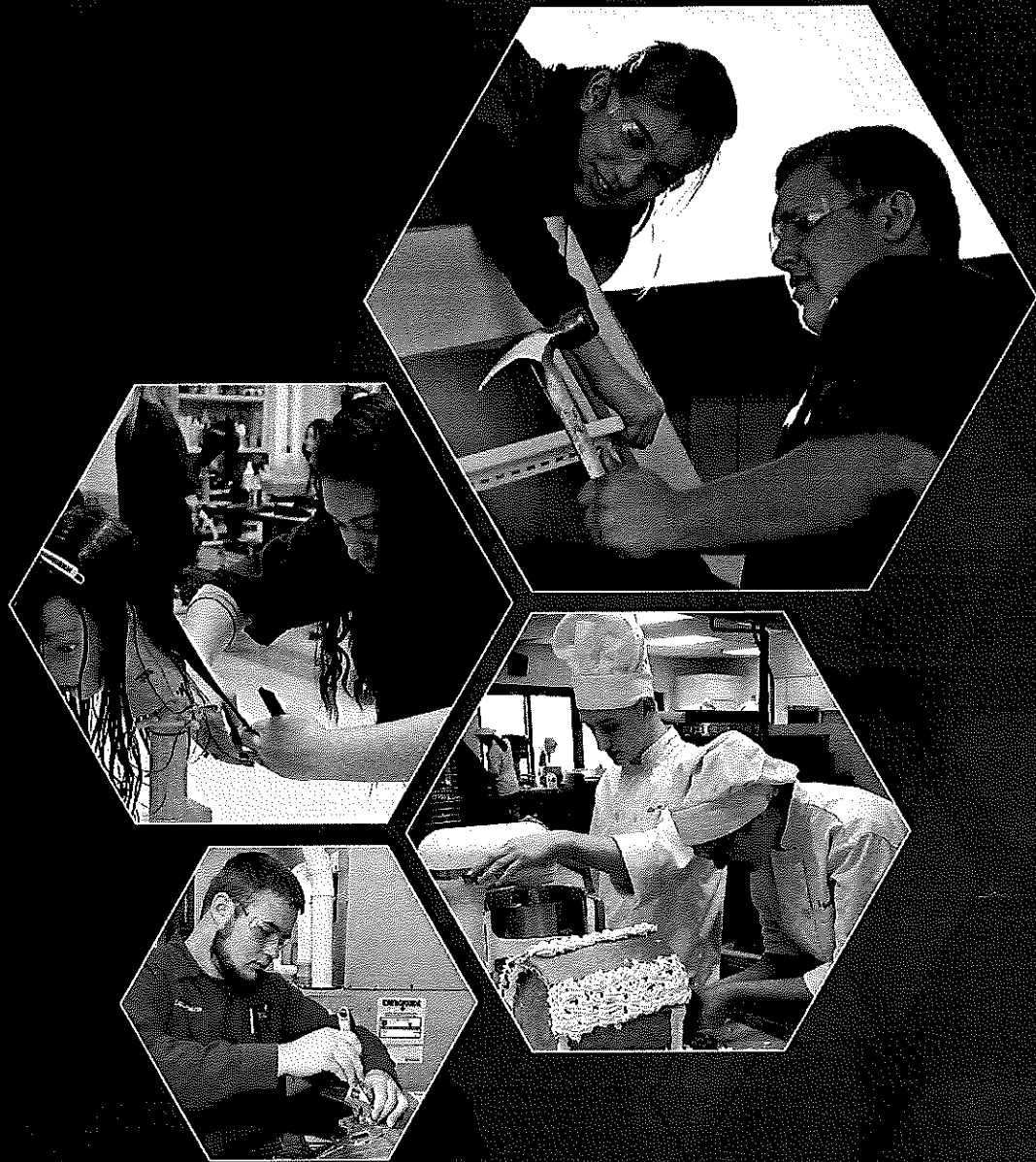
ADJOURNMENT

January 18, 2022

Date

Gretchen E. Wukits

Gretchen E. Wukits
Clerk of the Board



QUESTAR^{III}
PUTTING STUDENTS FIRST

Tech Valley High School:

FY 2020/21 Financial Risk Assessment

www.questar.org

TABLE OF CONTENTS

INHERENT RISK AREAS	1
ASSESSMENT OF RISK	2
PRIOR YEARS' COMMENTS AND RECOMMENDATIONS	3
ISSUES IDENTIFIED IN THE CURRENT YEAR	5
CLEARED COMMENTS	7

Inherent Risk Areas

Below are inherent risks that should be addressed as part of conducting the annual independent audit and the ongoing internal audit function:

RISK AREA	DESCRIPTION	RECOMMENDATION
Changing Environment	Tech Valley operates in an environment of complex or frequently changing compliance requirements. The risk to Tech Valley is that as compliance regulations change complexities place task burdens on Tech Valley employees. The complexity of the tasks increases the risk that Tech Valley could feel adverse consequences if it were to lose a key person in the business office.	To mitigate this risk, Tech Valley should continue the process of documenting all critical financial processes, such as payroll, purchasing, accounts payable and IT processes. These documents should be reviewed, tested, and updated as the processes change. In addition, employees should continue to be cross trained to cover all critical process during vacations, prolonged absences, or vacancies in financial positions.
Complex Transactions	The entity has a mix of program types funded by third parties that could motivate management to shift costs or manipulate accounting transactions.	This is always an area of inherent risk. Tech Valley's Internal Audit function should monitor practices that ensure that funding regulations are understood and complied with. In addition, a properly functioning claims auditing procedure will review the appropriateness of costs charged to the various programs.
Segregation of Duties	The segregation of duties is an issue within schools primarily due to limited staffing and/or changes to employee responsibilities. There may be instances where Tech Valley has risk exposure and no mitigating controls.	Segregation of duties issues can be addressed in several ways: • Tech Valley could reassign work so that checks and balances are put in place and no one person has a span of control that is too extensive; • Additional review procedures could be developed and implemented either at the beginning or end of the process; or • The involvement of the claims auditor or internal audit function could be increased.
Prior Audits	Internal Audit has performed the following audits that will require a follow-up: • FY 2018/19 - Payroll	The Board of Education (BOE) should consider having Internal Audit perform follow-up audits to ensure management corrective actions to audit observations are working effectively and efficiently.

FY 2020/21 Financial Risk Assessment for Tech Valley High School

Assessment of Risk

Below is an assessment of Tech Valley's internal controls for each functional area which are classified as low; moderate; or high risk. The assessment is based on the likelihood and impact that an unfavorable event would have on Tech Valley. The functions that we deemed to be high risk areas are critical to the operation of Tech Valley or are assets susceptible to misappropriation. In addition, this information may be used by the Board of Education for developing an audit plan for the upcoming year.

Functional Area	Risk Classification		Comments
	Prior Year	Current Year	
Cash – Business Office	Low	Low	
Cash – Lunch Program	N/A	N/A	Capital Region BOCES is the food service provider for Tech Valley for the fiscal year 2020/21
Cash – Extraclassroom Activities	Moderate	Low	Clubs have not been financially active in FY 20.21
Cash – Petty Cash	Low	Low/Moderate	No Board policy in place regarding petty cash
Accounts Receivable – General	Moderate	Moderate	
Accounts Receivable – Special Education	Moderate	Moderate	
Accounts Receivable – Medicaid	N/A	N/A	Tech Valley is not involved in the Medicaid process
State Aid	N/A	N/A	Tech Valley does not receive state aid
Banking	Low	Low	
Accounts Payable	Moderate	Moderate	
Payroll	Moderate	Moderate	
Human Resources	Low/Moderate	Low/Moderate	
Purchasing	Low/Moderate	Low/Moderate	
Fixed Assets Accountability	Moderate/High	Moderate	Tech Valley now has a central fixed asset inventory listing
Transportation Fuel	N/A	N/A	Tech Valley does not provide transportation services to students
Inventory – Transportation Parts & Supplies	N/A	N/A	Tech Valley does not have transportation services
Inventory – Lunch Program	N/A	N/A	Lunch program provided by Capital Region BOCES
Inventory – Operations & Maintenance	N/A	N/A	O&M is provided by the SUNY Polytechnic Institute
Inventory - Extraclassroom	Low	Low	
Facilities Usage	N/A	N/A	Tech Valley does not rent out facilities
Employee Benefits	Low	Low	
Employee Expense Reimbursements	Low	Low	
Information Systems	Moderate/High	Moderate/High	
Capital Projects	N/A	N/A	Tech Valley does not conduct capital projects
Budgeting	Low/Moderate	Low/Moderate	
Claims Auditing	Low/Moderate	Low/Moderate	

Prior Years' Comments and Recommendations

We noted the following issues within functional areas that could use improvement to their internal controls. The comments and recommendations provide a tool for management to assist in developing or maintaining a risk management system that mitigates risk to an acceptable level as determined by the Board of Education. The issues were identified from prior risk assessments and are summarized in the table below along with our recommendations.

AREA IMPACTED	DESCRIPTION	RECOMMENDATION
Accounts Payable	The accounts payable clerk has the ability to add new vendors into the WinCap system.	Tech Valley should revise the permissions in the WinCap system to prevent the ability of the accounts payable clerks to be able to add new vendors. In addition, Tech Valley should develop a policy that details the separation of duties between the two BOCES that jointly operate Tech Valley (Questar III BOCES and Capital Region BOCES).
	Updated March 2021: There has been no change from the prior year risk assessment.	
Banking	Tech Valley currently does not have a system of positive pay in place.	Tech Valley should implement controls over cash that will limit threats from outside the organization by establishing a positive pay system with the bank. This would require that the organization instruct the bank regarding the checks that it has issued and has authorized the bank to pay. To accomplish this, the organization would create an electronic file of checks issued that would include the amount, and check number. The bank would be required to refer to this list before they could clear a check from the organization's account. This control would limit the District's exposure to check raising and fraudulent checks being paid from the organization's funds.
	Updated March 2021: At the time of the risk assessment, the Tech Valley was in the process of interviewing as part of the request for proposal (RFP) process for new banking services. If the new bank is chosen and approved by the Operating Board, positive pay would be included as a service. In addition, the Treasurer reviews the bank account activity daily.	

FY 2020/21 Financial Risk Assessment for Tech Valley High School

AREA IMPACTED	DESCRIPTION	RECOMMENDATION
Extraclassroom Activities	Profit & Loss forms are not always utilized as recommended by NYSED for fundraising activities in Tech Valley.	Tech Valley's Extraclassroom clubs should ensure they are completing Profit & Loss statements as applicable.
	Updated March 2021: There has not been enough financial activity from the Extraclassroom clubs in fiscal year 2020/21 to be able to determine if the clubs are consistently completing profit & loss statements when applicable.	
Fixed Assets	There has not been a full physical inventory completed to account and track all fixed asset inventory. We noted assets are owned by either Questar III BOCES or Capital Region BOCES and each BOCES accounts for their assets on their own databases. There is no combined inventory listing of all inventory. In addition, a fixed asset listing is not provided to the principal of Tech Valley. The list of fixed asset items Tech Valley possess should be provided to the Principal, so the Principal is aware of the items on hand.	Tech Valley should complete a full physical inventory to account and track all inventory. Once there is a complete inventory listing of items, the list should be provided to the Principal.
	Updated March 2021: Questar III BOCES will be conducting a full physical inventory in the spring of 2021. Tech Valley now has a combined, central fixed asset listing which is managed by Questar III BOCES. The Principal of Tech Valley has not been provided a listing of the fixed assets.	
	Questar III BOCES Response: The Questar III Asset Management and Valuation Service has completed the re-inventory of the TVHS fixed assets. Fixed asset listings will be provided to the TVHS Principal annually upon re-inventory.	
Information Technology	The backup procedures for the WinCap system have not been tested by NERIC staff.	NERIC staff should test the backup procedures for WinCap to ensure information is being backed up correctly.
	Updated March 2021: NERIC staff noted there has not been specific testing of the WinCap system backup and restoration for Tech Valley. NERIC staff noted backup data has been restored for other school district's NERIC services, so NERIC is assured information would be able to be restored if the need ever occurred.	

Issues Identified in the Current Year

We noted the issues below within functional areas that could use improvement to their internal controls. The comments and recommendations provide a tool for management to assist in developing or maintaining a risk management system that mitigates risk to an acceptable level as determined by the Board of Education. The issues were identified from the **FY 2020/21** Risk Assessment and are summarized in the table below along with our recommendations.

AREA IMPACTED	DESCRIPTION	RECOMMENDATION
Operating Board Policies	During our review of the policies for banking, we noted the Operating Board has not established a policy for petty cash.	Tech Valley should take steps to develop a formal policy regarding petty cash and review it periodically for any changes or updates.
Information Technology	The SchoolTool system is not configured to prompt users to change their passwords. Users have not been required to change their passwords since beginning employment with Tech Valley.	The SchoolTool system that is managed by Questar III BOCES should be configured to require systematic password changes at least annually to ensure security of the system. For best practices, passwords should be complex in nature.
	Questar III BOCES Response: The Questar III Data Analyst Team will be working with its Information Technology Team to develop a protocol for appropriate password updates to the SchoolTool system.	
	During interviews with staff, we noted it has been established between Capital Region BOCES and Tech Valley that the Data Protection Officer for Tech Valley will be the same Data Protection Officer that was appointed for Capital Region BOCES, however, this individual was not formally approved by the Operating Board as Tech Valleys Data Protection Officer.	The Operating Board should approve the appointment of the Data Protection Officer. Per Education Law 2-D (Ed Law 2-D) section 121.8, "Each educational agency shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency." To ensure best practices, the Data Protection Officer should be appointed each year in the reorganizational meeting.
	The Parent's Bill of Rights was not published on Tech Valleys website. At the time of the risk assessment Tech Valley was in the process of determining a plan to comply with Ed Law 2-D section 121.3.	Per Ed Law 2-D: §121.3 Bill of Rights for Data Privacy and Security. (a) Each educational agency shall publish on its website a parent's bill of rights for data privacy and security ("bill of rights") that complies with the provisions of Education Law §2-d (3). (b).

FY 2020/21 Financial Risk Assessment for Tech Valley High School

AREA IMPACTED	DESCRIPTION	RECOMMENDATION
	Tech Valley does not have on their website a platform where parents can submit a complaint regarding a breach or unauthorized release of PII. At the time of the risk assessment, Tech Valley was in the process of determining a plan to include a platform on their website where parents can submit a complaint.	New York State Education Law 2-D section 121.4 (a) states that each educational agency must establish and communicate to parents, eligible students, teachers, principals, or other staff of an educational agency, its procedures for them to file complaints about breaches or unauthorized releases of student data.
	Tech Valley does not have on their website a listing of data inventory. At the time of the risk assessment Tech Valley was in the process of determining a plan to upload on the website all approved subscriptions and applications.	New York State Education Law Section 2-D requires that the State Education Department make publicly available on the department's website an inventory and understandable description of the student, teacher and principal data elements collected with an explanation and/or legal or regulatory authority outlining the reasons such data elements are collected and the intended uses and disclosure of the data. This table contains the inventory and a description of the data element.

Cleared Comments

The following comments and recommendations were identified from previous annual risk assessments but have been adequately addressed by the High School. This information is reporting for informational and historical purposes only.

AREA IMPACTED	DESCRIPTION	CORRECTIVE ACTION
Accounts Payable	There is no operational procedure in place for accounts payable process.	Updated March 2021: There is an operational procedure in place for the accounts payable process.
Banking	The petty cash funds issued were not approved by the Board of Education in the reorganizational meeting minutes.	Updated March 2021: The Petty cash fund was approved in the Operating Board's reorganizational meeting.
Extraclassroom	The Extraclassroom central treasurer is not approved by the Board of Education on an annual basis.	Updated March 2021: The Extraclassroom Central Treasurer was appointed by the Operating Board in the January 28, 2021 Operating Board minutes.
Information Technology	Tech Valley does not have a formal cybersecurity awareness training that is provided to all non-instructional and instructional staff. As a result, Tech Valley staff have limited knowledge regarding potential exposure to cyber threats or attacks.	Updated March 2021: As of the fall of 2020, all Tech Valley staff are required to take an online cybersecurity and awareness training. The training will be required to be taken by all staff on an annual basis. The training includes information on password security, personal emails, personal use of the internet, and personal identifiable information (PII). Tech Valley also has data protection Fridays where an informative newsletter is sent to all staff regarding information technology best practices and information.
	Tech Valley has not established a formal process in the event of a breach and/or unauthorized use of Personal Identifiable Information (PII).	Updated March 2021: Capital Region BOCES has established a formal written cyber security incident response plan that Tech Valley will follow. In addition, the high school has adopted board policies 8635 Information Security Breach and Notification and policy 8635-R Information Security Breach and Notification Regulation.



Date: October 20, 2021

From: John Mattox

To: Wendy Ashley

Subject: Response to the FY 2020/21 Risk Assessment

Inherent Risk Area

Changing Environment

Recommendation: *To mitigate this risk, Tech Valley should continue the process of documenting all critical processes, such as payroll, purchasing, accounts payable and IT processes. These documents should be reviewed, tested and updated as the processes change.*

In addition, employees should continue to be cross trained to cover all critical process during vacations, prolonged absences or vacancies in financial positions.

Management's Response: The procedures used to process the payroll, purchasing, accounts payable, Information Technology, and other business office function are the same as Capital Region BOCES. Employee are cross-trained to cover vacations and prolonged absences.

Complex Transactions

Recommendation: *This is always an area of inherent risk. Tech Valley's Internal Audit Function should monitor practices that ensure that funding regulations are understood and complied with.*

In addition, a properly functioning claims auditing procedure will review the appropriateness of cost charged to the various programs.

Managements Response: Tech Valley High School is just that, a high school. It does not have the same inherent risks as a normal K-12 school district has. A majority of the revenue is through student's tuition paid by the home BOCES and a NYS Grant.

Tech Valley High School has a properly functioning claims auditing process.

Segregation of Duties

Recommendation: *Segregation of duties issues can be addressed in several ways:*

- *Tech Valley could reassign work so that checks and balances are put in place and no one person has a span of control that is too extensive:*

- *Additional review procedures could be developed and implemented either at the beginning or the end of the process; or internal audit function could be increased.*

Management's Response: Tech Valley High School does have checks and balances to monitor all aspects of the business office.

Prior Audits

Recommendation: *The Board of Education should consider having the Internal Audit perform follow-up audits to ensure management corrective actions to audit observations are working effectively and efficiently*

Issues identified in the Prior Year:

Accounts Payable:

Recommendation: *Tech Valley should revise the permissions in the WinCap system to prevent the ability of the accounts payable clerks to be able to add new vendors. In addition, Tech Valley should develop a policy that details the separation of duties between the two BOCES that jointly operate Tech Valley.*

Management's Response:

Compensating controls considerations:

1. Purchasing Agent has to review documentation and approve the purchase and create a PO. Before the Purchasing Agent approving the PO, the chain of approvals from the administration at TVHS would also have had to take place.
2. If step #1 isn't followed, or the attempt to create a PO after a purchase has been made a PO exception report is created which has to be approved by an additional supervisor and is reported by the claims auditor in the claims auditor report to the Board.
3. The Claims Auditor reviews all claims and has extensive working knowledge of the claims and vendors common amongst school districts and questions vendors out of the ordinary. The Claims Auditor reviews the claims for remit address as well as agreement to the vendor address on the original PO.

We can also use a compensating control with a quarterly review by Tech Valley's Deputy Treasurer of the "Vendor Record Change Report" to reduce the risk of vendor information being changed.

Banking:

Recommendation: *Tech Valley should implement controls over cash that will limit threats from outside the organization by establishing a positive pay system with the bank. This would require that the organization instruct the bank regarding the checks that it has issued and has authorized the bank to pay. To accomplish this, the organization would create an electronic file of checks issued that would include the amount, and check number. The bank would be required to refer to this list before they could clear a check from the organization's account. This control would limit the District's exposure to check raising and fraudulent checks being paid from the organization's funds.*

Management's Response:

Tech Valley utilizes Payment Protection Service, a free service where you would go into Key Navigator daily, review the payment protection report for all checks presented for payment, any checks not issued by Tech Valley will be marked and returned, and all others will pay by default. It does have to be reviewed daily – the check list is available by 9am. If no one reviews the check list, ALL will pay at the 2pm deadline.

ExtraClassroom Activity Fund:

Recommendation: *Tech Valley's Extraclassroom clubs should ensure they are completing Profit & Loss statements as applicable.*

Management's Response: This is a good practice and will be reviewed for each club, however not required under the Regulations of the Commissioner. (8 NYCRR Part 172)



To: Tech Valley High School Board of Education
From: Capital Region BOCES
RE: Capital Region BOCES Response to the TVHS Risk Assessment Report
Date: January 19, 2022

TVHS 2020-2021 Risk Assessment Update

Background

Questar III BOCES Internal Audit Staff performed a risk assessment update of TVHS during the 2020-21 school year. The audit reviewed a majority of functions that are performed by the Business Office of Capital Region BOCES, which is also reviewed annually by an independent external audit firm. The Risk Assessment update contained several comments and recommendations to inherent risk, areas of risk identified in prior year reports, and current year issues.

We appreciate the observations and recommendations provided in the assessment, however there are concerns over the independence of the internal audit assessment and the method of evaluating some of the internal controls. A couple of recommendations for corrective action were for actions to be taken by Questar III BOCES. Since Questar III is also providing the internal audit service, this could create the appearance of a conflict.

A number of recommendations also appeared to be "boilerplate" comments without taking into consideration the relative size and scope of Tech Valley High School's operations. Many of the risks that are found at a usual school district are not present at Tech Valley due to its size and narrow operations.

During the evaluation of internal controls, it also appears the audit may have been an "audit by checklist" instead of taking the collection of preventative, detective, and compensating controls together to evaluate the "system" of internal controls. We believe if this approach had been taken, many recommendations could have been eliminated.

The recommendations and management's response to the recommendation are as follows. All recommendations were taken directly from the draft audit report as they appeared in the report.

Inherent Risk Area

Changing Environment

Recommendation: *To mitigate this risk, Tech Valley should continue the process of documenting all critical processes, such as payroll, purchasing, accounts payable and IT processes. These documents should be reviewed, tested and updated as the processes change.*

In addition, employees should continue to be cross trained to cover all critical process during vacations, prolonged absences or vacancies in financial positions.

Management's Response: Management believes we are constantly evaluating the changing environment. The procedures used to process the payroll, purchasing, accounts payable, Information Technology, and other Business Office functions are the same as Capital Region BOCES. Employees are cross-trained to cover vacations and prolonged absences.

During the past year, as a result of operating under COVID restrictions, these procedures were tested with personnel operating remotely and with different individuals performing some operations as a result of COVID vacancies/quarantines.

Complex Transactions

Recommendation: *This is always an area of inherent risk. Tech Valley's Internal Audit Function should monitor practices that ensure that funding regulations are understood and complied with.*

In addition, a properly functioning claims auditing procedure will review the appropriateness of cost charged to the various programs.

Management's Response: This recommendation is confusing since the recommendation is that the auditors writing the report are making a recommendation for them to continue to perform their duties to monitor.

This recommendation is additionally confusing. Based on the size and scale of Tech Valley High School, financial operations are much less complex than a normal K-12 school district. A majority of the revenue comes from student tuition paid by the home BOCES and a NYS grant. Many of the complexities involved with a public school district, such as a tax cap, and reserve calculations, are not present with TVHS.

Additionally, on the expenditure side of Tech Valley High School, there are also very limited complex transactions. For example, during the 2020-21 school year there were only 63 vendors paid through accounts payable with the top 10 vendors comprising over ninety percent of the expenses. Tech Valley High School has a limited number of complex transactions since many functions are outsourced to either Questar or Capital Region BOCES.

Tech Valley has a very experienced claims auditor and based on the limited number of vendors used by Tech Valley, is very aware of what normal operational expenses are and what vendors can be expected to be utilized.

Segregation of Duties

Recommendation: Segregation of duties issues can be addressed in several ways:

- Tech Valley could reassign work so that checks and balances are put in place and no one person has a span of control that is too extensive:
- Additional review procedures could be developed and implemented either at the beginning or the end of the process; or internal audit function could be increased.

Management's Response: Tech Valley High School does have checks and balances to monitor all aspects of the business office and we believe this risk has been significantly minimized with the design of the internal controls.

Prior Audits

Recommendation: The Board of Education should consider having the Internal Audit perform follow-up audits to ensure management corrective actions to audit observations are working effectively and efficiently.

Management's Response: There is no recommendation needed. The Board will continue to evaluate all audit areas each year when presented with the Risk Assessment. As part of the Board's responsibilities, the performance of operations is always being evaluated.

Issues identified in the Prior Year:

Accounts Payable:

Recommendation: Tech Valley should revise the permissions in the WinCap system to prevent the ability of the accounts payable clerks to be able to add new vendors. In addition, Tech Valley should develop a policy that details the separation of duties between the two BOCES that jointly operate Tech Valley.

Management's Response: We feel that due to the size and scope of Tech Valley High Schools vendors and that there are very few additions or deletions, we have significant compensating controls that significantly reduce the risk of fraud or impropriety. The compensating controls are:

1. The Purchasing Agent must review documentation, approve the purchase and create a purchase order. Before the Purchasing Agent approves the purchase order, the chain of approvals from the administration at TVHS would also have had to take place. If the Accounts Payable staff were to attempt fraud, collusion would have to involve the Accounts Payable clerk, the purchasing agent, the administrator at TVHS, and possibly the Claims Auditor to effectively commit fraud.
2. If step #1 isn't followed, or the attempt to create a purchase order after a purchase has been made, a purchase order exception report is created which has to be approved by an additional supervisor and as reported by the Claims Auditor in the Claims Auditor report to the Board. The dates of all POs and the dates of receipt of the product or service are reviewed by the Claims Auditor.
3. The Claims Auditor reviews all claims and has an extensive working knowledge of the claims and vendors commonly used by school districts and specifically Tech Valley High School. The Claims Auditor questions payment requests to vendors that are not ordinary. As part of the Claims Auditor review, the remit address as well as the vendor address on the original PO is reviewed.
4. We can also perform a quarterly review by Tech Valley's Deputy Treasurer of the "Vendor Record Change Report" to reduce the risk of vendor information being changed.

The control of preventing accounts payable staff from creating vendors is a recommended best practice in most sectors of business, however, most organizations do not have dedicated purchasing agents and claims auditors that are the internal control gatekeepers at the beginning and end of the transactions. We believe our process provides strong internal controls and reduces the need for additional personnel to input vendor file data, at an additional expense to the school.

As an additional consideration, this process for Tech Valley High School is the same process that is performed at Capital Region BOCES, with the same personnel. The independent internal and external auditors have reviewed this process and did not issue any findings or recommendations in their reports. This is significant since the risk, based on transaction volume and dollar amount far exceeds Tech Valley High School.

Banking:

Recommendation: *Tech Valley should implement controls over cash that will limit threats from outside the organization by establishing a positive pay system with the bank. This would require that the organization instruct the bank regarding the checks that it has issued and has authorized the bank to pay. To accomplish this, the organization would create an electronic file of checks issued that would include the amount, and check number. The bank would be required to refer to this list before they could clear a check from the organization's account. This control would limit the district's exposure to check-raising and fraudulent checks being paid from the organization's funds.*

Management's Response: Tech Valley utilizes "Payment Protection Service", a free service where you go into Key Navigator daily, review the payment protection report for all checks presented for payment, any checks not issued by Tech Valley will be marked and returned, and all others will pay by default. It does have to be reviewed daily – the checklist is available by 9 am. If no one reviews the check list, ALL items will pay at the 2 pm deadline.

We recognize that positive pay is ideal for organizations with a large volume of checks, but it comes with an expense from the bank. During the 2020-21 school year, Tech Valley High School issued only 147 accounts payable checks and less than 30 payroll checks. We believe that we have designed our internal controls in a manner that reflects the risk and is also cost-effective.

ExtraClassroom Activity Fund:

Recommendation: *Tech Valley's Extra-classroom clubs should ensure they are completing Profit & Loss statements as applicable.*

Management's Response: This is a good practice and will be reviewed for each club, however, this is not required under the Regulations of the Commissioner. (8 NYCRR Part 172)

Fixed Assets:

Recommendation: Tech Valley should complete a full physical inventory to account and track all inventory. Once there is a complete inventory listing of items, the list should be provided to the Principal.

(From the audit report...)

Updated March 2021: Questar III BOCES will be conducting a full physical inventory in the spring of 2021. Tech Valley now has a combined, central fixed asset listing which is managed by

Questar III BOCES. The Principal of Tech Valley has not been provided a listing of the fixed assets.

Questar III BOCES Response: The Questar III Asset Management and Valuation Service has completed the re-inventory of the TVHS fixed assets. Fixed asset listings will be provided to the TVHS Principal annually upon re-inventory.

Management's Response: As noted in the above response, Questar III BOCES, the same organization performing the internal audit, has performed the inventory. This should resolve this deficiency.

Information Technology:

NERIC staff should test the backup procedures for WinCap to ensure information is being backed up correctly.

(From the audit report...)

Updated March 2021: NERIC staff noted there has not been specific testing of the WinCap system backup and restoration for Tech Valley. NERIC staff noted backup data has been restored for other school district's NERIC services, so NERIC is assured information would be able to be restored if the need ever occurred.

Management's Response: Although not specific to Tech Valley High School, NERIC has an IT audit performed by external independent IT auditors which examine backup procedures.

Issues Identified in the Current Year:

Operating Board Policies:

Recommendation: Tech Valley should take steps to develop a formal policy regarding petty cash and review it periodically for any changes or updates.

Management's Response: The Board will update its policies to include a petty cash policy during the 2022 school year.

Information Technology:

Recommendation: The SchoolTool system that is managed by Questar III BOCES should be configured to require systematic password changes at least annually to ensure security of the system. For best practices, passwords should be complex in nature.

(From the audit report...)

Questar III BOCES Response: The Questar III Data Analyst Team will be working with its Information Technology Team to develop a protocol for appropriate password updates to the SchoolTool system.

Management's Response: As noted this corrective action will be addressed by Questar III BOCES, the same organization that performed the internal audit.

Data Protection Recommendations:

1. The Operating Board should approve the appointment of the Data Protection Officer. Per Education Law 2-D (Ed Law 2-D) section 121.8, "Each educational agency shall designate a Data

Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law § 2-d and this Part, and to serve as the point of contact for data security and privacy for the educational agency.” To ensure best practices, the Data Protection Officer should be appointed each year in the reorganizational meeting.

2. Per Ed Law 2-D: §121.3 Bill of Rights for Data Privacy and Security. (a) Each educational agency shall publish on its website a parent’s bill of rights for data privacy and security (“bill of rights”) that complies with the provisions of Education Law § 2-d (3). (b).
3. New York State Education Law 2-D section 121.4 (a) states that each educational agency must establish and communicate to parents, eligible students, teachers, principals, or other staff of an educational agency, its procedures for them to file complaints about breaches or unauthorized releases of student data.
4. New York State Education Law Section 2-D requires that the State Education Department make publicly available on the department’s website an inventory and understandable description of the student, teacher and principal data elements collected with an explanation and/or legal or regulatory authority outlining the reasons such data elements are collected and the intended uses and disclosure of the data. This table contains the inventory and a description of the data element.

Management’s Response: The Operating Board and Tech Valley High School Administration will implement the requirements to comply with the appointment and disclosures required to comply with Ed Law 2D, during the 2022 school year.

Final Observation: Every organization needs to design a system of internal controls that fits the organization’s size and scale to achieve a balance of risk and expense. We believe we have designed an internal control structure that minimizes risk to an acceptable level. No two internal control structures are going to be designed the same and therefore the audits of internal controls should also be designed to view the entire system of internal controls.



QUESTAR^{III}
PUTTING STUDENTS FIRST

Tech Valley High School:
FY 2020/21 Information Technology

www.questar.org



July 23, 2021

Board of Education
Tech Valley High School
246 Tricentennial Drive
Albany, New York 12203

We have completed the annual testing of controls for Tech Valley High School. Our engagement was designed to evaluate the adequacy of internal controls over the Information Technology process to ensure they are appropriately designed and operating effectively and efficiently. And, to provide a report with recommended changes for strengthening controls and reducing identified risks.

The purpose of the audit was to review the internal controls that the school has in place to prevent errors, detect fraud and ensure that financial reporting is accurate and that the school assets are safeguarded.

RELIABILITY OF INFORMATION

As noted, the purpose of our engagement was to assist you in improving the process by which you monitor and manage the risks that face the school. Any findings and recommendations in the attached report are the responsibility of the school to implement, accept the risk as identified, or implement alternative controls that will mitigate the risk to a level that is acceptable by the school. Ultimately, it is your responsibility to assess the adequacy of your risk management system.

DISTRIBUTION OF THE REPORT

This report is intended solely for the information and use of the Board of Education and management of Tech Valley High School and should not be used for any other purpose.

We appreciate the opportunity to serve you and thank the individuals in your organization for their cooperation. Over time, it will be necessary to reassess your risks to ensure that they have not changed and to ensure that your risk management system is functioning properly. Through our ongoing involvement with you as a client and our knowledge of your school and its processes, we are in a unique position to assist you with that process. Please contact us at any time should you desire such services.

Sincerely,

Mark Beaudette
Internal Audit Manager
Questar III

REPORT TO THE BOARD OF EDUCATION

Executive Summary**Objectives and Scope**

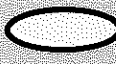
The Tech Valley Operating Board has asked us to examine Tech Valley's IT process. Key objectives include evaluating whether or not Tech Valley is receiving the Cooperative Technology Services from NERIC.

Our fieldwork concluded on July 23, 2021.

For the audit we interviewed various staff members from the Northeastern Regional Information Center (NERIC) and from Tech Valley to gain information about the IT process. In addition, we tested a sample of 35 help desk tickets to ensure tickets are being closed timely. We also reviewed a visitor log Tech Valley maintains to ensure a NERIC technician is onsite one day per week from September 2020 – June 2021.

Conclusion

Three observations were noted and are summarized below. Our recommendations are detailed in the report.

Reference	Observation	Risk	
1	7 out of 42 weeks where there was no evidence of NERIC staff being on site at TVHS		Medium
2	13 out of 35 help desk tickets tested were not closed timely		Medium
3	Two factor authentication has not been implemented for staff email nor google drive		Low

FY 2020/21 TECH VALLEY HIGH SCHOOL INFORMATION TECHNOLOGY AUDIT REPORT

ENTITY NAME	Tech Valley High School
REPORT DATE	July 23, 2021
PROCESS REVIEWED	Information Technology
PERSONNEL INTERVIEWED	Dr. Amy Hawrylchak, Chief Academic Officer/Principal (TVHS) Sarah Fiess, School Outreach Coordinator (TVHS) David Versocki, Chief Technology Officer (NERIC) Michael Olson Jr, Technology Operations Manager (NERIC) Kevin Kerr, Management Program Coordinator II (NERIC)
SCOPE OF WORK	We reviewed the information technology policies and procedures and conducted interviews with key personnel from Questar III BOCES, NERIC, and Tech Valley to obtain an understanding of the process. From a population of 299 help desk tickets that were issued from Tech Valley from November 1, 2019 – October 31, 2020, we randomly selected 35 tickets to test to ensure help desk tickets are being closed in a reasonable, timely manner. Reviewed a badge log in report which notes the dates and times a NERIC staff member who mainly services Tech Valley entered Tech Valley's building. We reviewed the log and tested all weeks from February 2021 – June 2021 to ensure a NERIC staff member was on site at least one day per week per the Cooperative Technology Services bill for Tech Valley. Additionally, since there was no badge log available before February of 2021, we reviewed the physical visitor sign in sheets at tech valley as well as the Tech Valley app report logs for all weeks between September 2020 – January 2021. Reviewed all items (6) that were purchased through NERIC for Tech Valley to ensure NERIC is providing purchasing services.
SCOPE RESTRICTIONS	None noted.
AUDIT OBJECTIVES	• Evaluate the efficiency and effectiveness of the Information Technology process; • Determine the existence and effectiveness of the system of internal controls over Network Security; • Evaluate if the high school is receiving the necessary support from NERIC, • Provide recommendations to help mitigate any identified risks.
KEY PROGRAM CONTROLS	The High School has created the following key program controls designed to meet business obligations, provide accountability, and promote operational effectiveness & efficiencies:

FY 2020/21 TECH VALLEY HIGH SCHOOL INFORMATION TECHNOLOGY AUDIT REPORT

	• Tech Valley receives Cooperative Technology Services (CTS) from NERIC. These services provide tech support to Tech Valley and include but are not limited to: an onsite help desk technician one day per week, procurement services, ServiceNow enterprise Service Management Platform implementation, and additional on-site and remote support as needed. • The Technical Operations Manager of NERIC and the Tech Valley Principal hold weekly meetings to discuss IT related items such as technology goals and initiatives as well as budgeting and project status. • NERIC has protections on Tech Valley's network and various forms of intrusion detection. NERIC also has a firewall to protect Tech Valley's network from other Districts. NERIC also offers Denial Service Attack protection that protects the internet connection. • Staff at the high school use cloud-based services to access documents such as Google and ECHO Cloud Solutions. These systems are both encrypted. • When staff use the internet, they use hypertext transfer protocol secure (HTTPS). In HTTPS, the communication protocol is encrypted using Transport Layer Security. • Each staff member is issued a Windows device. These devices have end user encryption via a bit locker encryption. This is disk level encryption. In addition, the cell phones that are issued to staff members are encrypted and passcode protected.
OBSERVATIONS AND RECOMMENDATIONS	<u>Observation 1:</u> During our review of the visitor sign in logs, the app report logs, and the badge log in report, we noted for 7 out of 42 weeks tested there was no evidence of NERIC staff being on site at Tech Valley. During conversations with staff, we noted NERIC does not have a system in place to ensure the Technician is where they are supposed to be and there is no log maintained as to who was on site. In addition, we noted various instances where the NERIC help desk technician did not sign in/badge in on time in the morning, but the individual is supposed to on site one full day (8 hours including a half hour lunch) per week per the Cooperative Technology Service Description. <i>Recommendation: NERIC should develop a formal log to keep track of TECH's who are out in the field. NERIC should ensure there is a technician on site at Tech Valley at least one full day per week per the Cooperative Technology Service they provide to Tech Valley.</i> <u>Observation 2:</u> During our testing of 35 help desk tickets, we noted 13 instances where NERIC was not timely in closing help desk tickets. These instances ranged from 6 to 205 days from the date the ticket was opened to the date the ticket was closed. We also noted instances where technicians are not putting detail notes in the tickets to note when they address the ticket and give updates to the requestor on the status of the ticket. According to the NERIC Service Level Description for Cooperative Technology Services page 3, the target incident resolution schedule is that less than 5 business days 75%

FY 2020/21 TECH VALLEY HIGH SCHOOL INFORMATION TECHNOLOGY AUDIT REPORT

	of incident tickets will be resolved. For request tickets it notes the resolution time is dependent upon a number of factors that includes the scope and nature of the request, so a target request resolution is fluid. In addition, during conversations with the Tech Valley staff they noted tickets are not always addressed timely. One staff noted if they submit a ticket for a broken computer, it will go unaddressed for months; and that there are times where a ticket is noted as moderate or high urgency, but it is still not addressed timely. <i>Recommendation: NERIC should devise a formal process on ensuring they are answering help desk tickets in a timely manner. In addition, NERIC should provide training to all Technicians that are assigned to resolve help desk tickets. The training should include methods to maximize documentation of valuable detail in the tickets and to ensure that the tickets are addressed as soon as possible.</i> <u>Observation 3:</u> Tech Valley does not have implemented two factor authentication for staff to log onto their email nor Google drive or Google classroom. Implementing two factor authentication could secure user logins from attackers who exploit weak log in credentials. <i>Recommendation: Tech Valley should consider implementing two factor authentication log in for staff for their email and Google drive. Tech Valley should decipher whether or not they would have staff use their cell phone or a token for two factor authentication.</i>
SUBMITTED BY:	Alexa Schaefer, Internal Auditor
DATED:	July 23, 2021



To: Tech Valley High School Board of Education
From: Capital Region BOCES
RE: Capital Region BOCES response to TVHS 20-21 Information Technology Audit-
 Report date: July 23, 2021 for Fiscal Yr 20-21
Date: January 19, 2022

Background

Questar III BOCES Audit staff conducted a Risk Assessment of Tech Valley High School (TVHS) which resulted in an internal audit of Capital Region BOCES technology support services provided to the Tech Valley High School. The purpose of the engagement was to evaluate the adequacy of internal controls over information technology process to ensure they are properly designed and operating effectively and efficiently.

The audit report contains three (3) observations and recommendations, summarized as follows:

#1 Observation and Recommendation

Observation Summary:

Capital Region BOCES IT staff attendance at TVHS.

- a. Audit staff reviewed a 42-week period and found that CR BOCES IT staff was not on site 7 out of the 42 weeks.
- b. NERIC does not have a system in place to ensure the attendance of the assigned technician.
- c. The assigned NERIC IT technician did not sign in or badge in on time "various" instances. According to the Cooperative Service Agreement the assigned technician is supposed to be on site one full day per week (8 hours per day).

Audit Recommendation:

NERIC should develop a formal log to keep track of IT staff who are out in the field. NERIC should ensure there is a technician on site at TVHS at least one per week.

#2 Observation and Recommendation

Observation Summary:

Help Desk tickets and response for support.

- a. Audit staff review 35 service tickets. There were 13 instances where tickets were not closed timely.
- b. Instances were identified where there was insufficient detail notes in the ticket to indicate when they address the issue and update the requestor.
- c. TVHS staff noted that tickets are not always addressed timely.

RE: TVHS 20-21 Information Technology Audit- Report date: July 23, 2021 for Fiscal Yr 20-21

Audit Recommendation:

NERIC should devise a formal process to ensure they are answering help desk tickets in a timely manner and provide training to all technicians assigned to resolve tickets. Training should include methods to maximize documentation of valuable detail in tickets and to make sure issues are addressed timely.

#3 Observation and Recommendation

Observation Summary:

TVHS has not implemented two-factor authentication

a.) There is no two-factor authentication for email, Google drive or Google classroom

Audit Recommendation:

TVHS should consider implementing two factor authentication for staff email and Google drive. TVHS should also consider if they would have staff use their cell phone or a token for authentication.

Capital Region BOCES Response

The Capital Region BOCES has several concerns regarding the Risk Assessment and Internal Audit. Our concern and response centers on the following areas:

- Independence and Objectivity
- Focus, Scope and Necessity of the Internal Audit
- Response to Audit Observations and Recommendations.

Independence and Objectivity

One of the central tenants of an audit function is the notion of independence and objectivity. Governmental Auditing Standards and the Institute for Professional Practice of Internal Auditors and the NYS Education Department have outlined recommended relationship standards to ensure independence and objectivity and to prevent the appearance of a conflict of interest.

There are several relational circumstances that are present in the operation of the Tech Valley High School that could be construed to be in contravention of best practice standards for independence and objectivity as it relates to TVHS. Below are examples of this:

- Tech Valley High School ("TVHS") is a joint program combining both Questar III BOCES and Capital Region BOCES. TVHS's Board and the management decisions for the program are made up of members from both BOCES. Since the internal audit function is a service within Questar BOCES, it is questionable if a level of independence can be maintained in regard to operations managed and/or decisions made by Questar management with respect to TVHS.
- Internal Audit guidelines published by the New York State Education Department state that BOCES are not allowed to be the internal auditor to their component schools. Although TVHS is not a

RE: TVHS 20-21 Information Technology Audit- Report date: July 23, 2021 for Fiscal Yr 20-21

component school, it operates in an substantial position of influence in this setting as Questar is significantly involved in the management of the school.

The current year's risk assessment report identifies deficiencies that have management responses supplied by Questar. This alone would send up a red flag to the State Education Department or the NYS Comptroller's Office, since Questar is essentially auditing themselves in this matter and the management of Questar is responding to the internal audit service operated by Questar.

Focus, Scope and Necessity of the Internal Audit

Internal Audits in NYS public schools were first legislated in 2005 as part of the NYS State budget in response financial malfeasance and incompetence occurring at school districts across the state.

The legislation and subsequent requirements in the Comptroller's five-point plan were focused on improving financial controls for school districts and BOCES at the organization or entity level. In response boards of education created audit committees to oversee the assessment process and to select areas of audit based on the level of level of risk.

Since 2005 legislation stipulating who is required to maintain an internal audit function also changed. Currently school districts who employ less than 8 teachers, have less than \$5 million in expenditures OR have fewer that 1,500 enrolled students are NOT required to maintain an internal audit function.

- TVHS is a BOCES program operated jointly by two BOCES and operates in much the same way as all BOCES instructional programs. It is not a "school district", it is a high-school level BOCES program, therefor there is no requirement to maintain or have an internal audit function. Districts elect to participate and send students and are charged a tuition similar to Career and Technical Education programs. Budgets are developed based on program needs and tuition is set based on the revenues needed to balance the budget. Thus, the internal audit in this context is analogous to conducting an internal audit of a specific BOCES program.
- The internal audit function has always been intended to focus on internal control structures related finances, NOT technology. The risk assessment and audit scope related to information technology has been added to the financial controls scope. An assessment of IT controls should be conducted as an IT audit or assessment, using audit or assessment frameworks specific to information technology such as NIST CSF. This audit was conducted under the guise of a financial controls framework, not an IT assessment framework
- The scope focused primarily on a self-selected service performance criteria used to evaluate NERIC staff. There appears to be little to no focus on IT practices associated with security practices or school operations where technologies are present, such as the its' use in instructional programming.

RE: TVHS 20-21 Information Technology Audit- Report date: July 23, 2021 for Fiscal Yr 20-21

- An Internal Audit usually involves a risk assessment and then a selected “focus area”. However, the review of the risk assessment and the selection of the focus area is usually performed the Board or the Board’s Audit Committee. During the past year’s review, it appears that the Risk Assessment results were not discussed with the TVHS Board or Audit Committee, and it also appears that the Board or Audit Committee did not select of the audit focus area. Usually, the area selected is an area of significant risk. This audit was essentially an audit of services by the other BOCES that jointly manages TVHS. This would appear to be a conflict by having one arm of management, auditing the other managing group. Again, creating perceptions of a lack of independence.
- As a matter of law each of the BOCES conducts an annual assessment and internal audit of their own financial operations as well external audits of financial operations. The audit of an internal BOCES program, such as TVHS, creates unnecessary redundancy and expense for both organizations.

Response to Audit Observations and Recommendations

In response to the three observations and recommendations appearing in the audit;

- NERIC support to TVHS is a cooperative IT support model. Meaning that the TVHS IT needs are supported through a team of technicians. Service is not delivered and built to be located “on site”, to support the needs of TVHS, therefor the observation and recommendation related to NERIC staffing presence, is not an indicator of a lack of support but a reflection of the manner in which the cooperative technology service is executed. Supports included in the service are:
 - Onsite staff as needed (tentative “day” to be onsite to handle physical tickets.
 - Check-ins with Technical Operations Manager regarding problems and projects.
 - Central site support from Network and Server Support teams (monitoring, break fix and project planning support).
 - Overall staff resources that can assist with TVHS needs is 20+ staff as part of this service.
 - Security tool licensing and support (CrowdStrike and Umbrella).
- During the audit period NERIC staff responded to 298 requests for support and closed 275 tickets. 23 remained open after the audit period as they were part of a longer term remediation issue. Additionally, NERIC staff have been reminded of the need to complete service tickets timely and in a complete manner providing adequate notes in the ticket.
- The lack of two-factor authentication is a responsibility of the administration of TVHS not NERIC staff. NERIC staff can assist in the implementation of this control but this needs to be an initiative directed by the administrative leadership at TVHS.

RE: TVHS 20-21 Information Technology Audit- Report date: July 23, 2021 for Fiscal Yr 20-21

In closing, the TVHS Board should consider the value and efficacy associated with maintaining an internal audit function. If there is a decision to continue an internal audit program for TVHS, its structure and focus should be jointly decided by the TVHS Board of Education.

**Audits Completed at other Districts:**

- Human Resources
- Purchasing
- Staff Attendance
- Fixed Assets Inventory
- Information Technology Inventory
- Claims Auditing
- Extraclassroom
- Cash Receipts/Disbursements
- Accounts Payable
- Payroll
- Information Technology



TECH VALLEY HIGH SCHOOL
INTERNAL CLAIMS AUDIT REPORT
Nov - Dec 2021

Warrant #	Description	Check Dates	Amount	Checks Issued	EFT's	Check Series
25	General Payable	11/3/2021	\$ 48,260.06	2	0	4582-4583
26	Federal	11/3/2021	\$ 17,292.00	1	0	4584
27	Payroll Deductions	11/10/2021	\$ 18,137.53	2	7	11349-11350
28	Payroll Deductions	11/24/2021	\$ 18,855.16	2	7	11352-11353
29	General Payables	11/24/2021	\$ 48,613.25	7	0	4585-4591
30	Extra-classroom	11/24/2021	\$ 250.00	1	0	1058
31	T&A Misc.	11/24/2021	\$ 5,542.08	1	0	11354
32	General Payables	12/1/2021	\$ 16,879.00	1	0	4592
33	Payroll Deductions	12/8/2021	\$ 18,429.11	2	7	11357-11358
34	Payroll Deductions	12/22/2021	\$ 18,313.44	2	7	11361-11362
35	General Payables	12/22/2021	\$ 52,304.62	12	0	4593-4604
36	T&A Misc	12/22/2021	\$ 5,542.08	1	0	11363
Period Totals			\$ 268,418.33	34	28	

Exceptions:	Warrant	Amount	Vendor	Explanation
None				

Michael Wolff

Michael T. Wolff, C.I.A.
Internal Claims Auditor
Tech Valley High School

January 3, 2022

TECH VALLEY HIGH SCHOOL
2021/2022 BUDGET
as of December 31, 2021

	ACTUAL RESULTS 2020/2021	APPROVED BUDGET 2021/2022	ACTUAL Budget 2021/2022
REVENUES			
Estimated Number of Students	132	130	130
Tuition	2,125,000	1,787,500	1,787,500
Tuition Other BOCES	0		
Tuition Non-Component	47,223	31,860	31,860
Special Education Billing	-	250,000	250,000
Legislative Grant #1	460,666	460,666	460,666
Legislative Grant Indirect		17,292	17,292
Revenue for Carry Over Encumbrance	73,052		68,115
Refunds Prior Years Expenses	314		
Tech Valley High School Foundation	-	15,000	15,000
Miscellaneous Revenue	25,213	5,000	5,000
Fund Balance		104,304	104,304
Contributed Rent			695,951
Interest Income	96	100	100
TOTAL REVENUES	2,731,564	2,671,722	3,435,788

TECH VALLEY HIGH SCHOOL

2021/2022 BUDGET

as of December 31, 2021

ACTUAL RESULTS 2020/2021	APPROVED BUDGET 2021/2022	ACTUAL Budget 2021/2022
--------------------------------	---------------------------------	-------------------------------

EXPENSES

ADMINISTRATIVE

Personnel

Administrative Salaries	59,100	118,000	118,000
Support & Clerical Salaries	52,540	54,384	54,384
Fringe Benefits	63,391	88,857	88,857
	<u>175,031</u>	<u>261,241</u>	<u>261,241</u>

Equipment

Equipment	35,693	10,000	20,500
-----------	--------	--------	--------

Materials & Supplies

General Supplies	12,000	10,000	10,000
Periodicals	-	500	500
Assets under \$500	1,000	1,000	1,000
Meeting Expenses/Food & Grocery	1,000	-	-
Subscriptions	350	250	250
Software Licenses	5,600	4,500	4,500
	<u>19,950</u>	<u>16,250</u>	<u>16,250</u>

Contractual

Telephone	7,005	9,605	9,605
Equip Repair and Maint	12,926	-	3,120
OTHER Operations & Maint	2,150	-	2,148
Insurance	45,466	47,466	46,666
Equip Rentals & Leases/ Hardware Software Rental	6,181	-	34,305
Postage	1,600	1,000	1,000
Travel-In-District	385	1,000	1,000
Conference & Other Travel	593	5,000	3,000
Assoc Dues & Memberships/Staff Dev	13,000	12,000	14,800
Printing & Copying	500	1,000	1,000
Workshop Related Costs	250	250	250
Other Misc Expense	5,180	5,000	5,000
Contributed Rent	-	-	695,951
Other Rental of Facility	84,120	86,700	86,700
	<u>179,256</u>	<u>169,021</u>	<u>904,545</u>

Contract Prof Service

External Accountants & Auditors	17,115	7,898	15,730
Funding Initiatives	17,292	17,292	17,292

Other Prof & Tech

	433	-	-
	<u>34,840</u>	<u>25,190</u>	<u>33,022</u>

School Districts & Other BOCES

BOCES/SCH DST -OTHER SRV	149,119	99,195	38,532
	<u>149,119</u>	<u>99,195</u>	<u>38,532</u>

Occupancy

TECH VALLEY HIGH SCHOOL

2021/2022 BUDGET

as of December 31, 2021

	ACTUAL RESULTS 2020/2021	APPROVED BUDGET 2021/2022	ACTUAL Budget 2021/2022
Data Communications	8,855	8,755	19,345
Cleaning/Ancillary Lease costs	8,855	8,755	19,345
TOTAL ADMINISTRATIVE	602,744	589,652	1,293,435

TECH VALLEY HIGH SCHOOL

2021/2022 BUDGET

as of December 31, 2021

ACTUAL RESULTS 2020/2021	APPROVED BUDGET 2021/2022	ACTUAL Budget 2021/2022
--------------------------------	---------------------------------	-------------------------------

INSTRUCTIONAL

Personnel

Instructional Salaries	1,047,223	1,082,422	1,095,427
Instructional Support Salaries	214,183	182,076	180,104
Substitute Teacher Salaries	9,940	2,500	3,550
Instructional Authorizations	-	-	2,302
Non-Instructional Salaries	43,503	45,729	47,729
Non Inst Auth	-	-	16,415
Fringe Benefits	534,865	572,440	570,347
	<u>1,849,714</u>	<u>1,885,167</u>	<u>1,915,874</u>

Equipment

Equipment	117,632	40,000	93,499
	<u>117,632</u>	<u>40,000</u>	<u>93,499</u>

Materials & Supplies

Supplies	23,470	15,000	8,000
Textbooks	2,500	8,000	4,307
Assets under \$500	-	1,000	1,000
Software Licenses	8,000	10,640	4,220
	<u>33,970</u>	<u>34,640</u>	<u>17,527</u>

Contractual

Postage	1,000	-	-
Hardware Software Rental	-	-	42,480
Travel Exp Business	-	-	500
Staff Development & Conferences Travel	300	4,200	700
Admissions	1,300	3,200	1,200
Transportation	-	10,500	3,500
Physical Education-Related Expenditures	-	2,000	178
Food Service	59,962	50,000	50,000
Misc	3,800	3,000	3,000
	<u>66,362</u>	<u>72,900</u>	<u>101,558</u>

BOCES/SCH DST -OTHER SRV

	28,858	49,396	13,896
	<u>2,096,536</u>	<u>2,082,103</u>	<u>2,142,353</u>

TOTAL PROGRAM COSTS

	<u>2,699,280</u>	<u>2,671,755</u>	<u>3,435,788</u>
--	------------------	------------------	------------------

COST PER STUDENT

	\$ 20,449	\$ 20,552	\$ 26,429
--	-----------	-----------	-----------

SURPLUS OR (DEFICIT)

	\$ 32,284	\$ (33)	\$ (0)
--	-----------	---------	--------

Date

Date

Treasurer

Finance Specialist II

TECH VALLEY HIGH SCHOOL
CONSOLIDATED REVENUE STATUS REPORT
as of 12/31/21

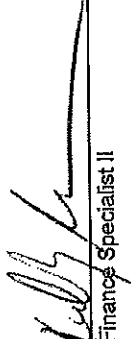
	Original Estimate	Adjustments	Current Estimate	Year-to-Date Revenues	Anticipated Balance
Anticipated Revenues					
Tuition A455	1,787,500.00		1,787,500.00	715,000.00	1,072,500.00
Tuition Other BOCES A455	0.00		0.00		0.00
Tuition Non Component A455	31,860.00		31,860.00	5,827.14	25,032.86
Special Education Billing	250,000.00		250,000.00	58,444.20	191,555.80
Legislative Grant 2021/2022 F904	460,666.00		460,666.00	115,166.00	345,500.00
Legislative Grant Indirect	17,292.00		17,292.00	17,292.00	0.00
TVHS Foundation	15,000.00		15,000.00		15,000.00
Revenue for Carry Over Encumbrance	0.00	68,115.00	68,115.00	68,115.00	0.00
Refunds of Prior Years Expense	0.00		0.00	7,220.38	-7,220.38
Gifts and Donations	0.00		0.00		0.00
Miscellaneous Revenue	5,000.00		5,000.00	19,741.00	-14,741.00
Fund Balance	104,304.00		104,304.00		104,304.00
Contributed Rent	695,951.00		695,951.00	294,619.28	401,331.72
Interest Income	100.00		100.00	43.46	56.54
Total Anticipated Revenues	3,367,673.00	68,115.00	3,435,788.00	1,302,468.46	2,133,319.54

HIGHLIGHTS/CHANGES

1/6/22
Date


Treasurer

1/6/22
Date


Financial Specialist II

TECH VALLEY HIGH SCHOOL CONSOLIDATED BUDGET STATUS REPORT

12/31/21

Description	Initial Budget		Adjustments		Current Budget		Year-to-Date Expenditures		Encumbrances Outstanding		Unencumbered Balance	
150 CERTIFIED SALARIES												
TEACHER SALARIES	1,084,922.00		15,357.00		1,100,279.00		554,562.31		545,067.06		649.63	
ADMINISTRATIVE SALARIES	300,076.00		(1,222.00)		298,854.00		149,426.94		149,426.81		0.25	
150 Subtotal Certified Salaries	1,384,998.00		14,135.00		1,399,133.00		703,989.25		694,493.87		649.88	
160 SUPPORT SALARIES												
160 Subtotal Support Salaries	100,113.00		17,665.00		117,778.00		62,824.54		54,951.67		1.79	
200 EQUIPMENT												
200 Subtotal Equipment	50,000.00		63,999.00		113,999.00		59,420.00		20,327.84		34,251.16	
300 SUPPLIES & MATERIALS												
GENERAL SUPPLIES	25,000.00		(6,000.00)		19,000.00		3,866.02		7,574.17		7,559.81	
TEXTBOOKS	8,000.00		(3,693.44)		4,306.56		2,802.94		89.90		1,413.72	
PERIODICALS	500.00		0.00		500.00		0.00		0.00		500.00	
ASSETS UNDER 500	2,000.00		0.00		2,000.00		219.99		0.00		1,780.01	
CAFETERIA (FRL)	50,000.00		0.00		50,000.00		9,000.00		41,000.00		0.00	
SUBSCRIPTIONS	250.00		0.00		250.00		0.00		0.00		250.00	
COMPUTER SOFTWARE PURCH	15,140.00		(6,420.00)		8,720.00		4,220.00		0.00		4,500.00	
300 Subtotal Supplies & Materials	100,890.00		(16,113.44)		84,776.56		20,108.95		48,664.07		16,003.54	
400 CONTRACTUAL & OTHER												
TELEPHONE	9,605.00		0.00		9,605.00		0.00		7,347.39		2,257.61	
DATA COMMUNICATIONS	8,755.00		10,590.00		19,345.00		12,986.05		6,355.38		3.57	
EQUIP REPAIR & MAINT	0.00		3,120.00		3,120.00		1,300.00		1,820.00		0.00	
OTHER O&M	0.00		2,148.00		2,148.00		0.00		2,148.00		0.00	
INSURANCE	47,466.00		(800.00)		46,666.00		44,503.00		200.00		1,963.00	
HARDWARE/SOFTWARE RENTAL	1,000.00		76,785.00		76,785.00		46,533.27		30,249.67		2.06	
POSTAGE	1,000.00		0.00		1,000.00		216.37		783.63		0.00	
TRAVEL-IN DISTRICT	1,000.00		500.00		1,500.00		243.60		256.40		1,000.00	
CONFERENCE & OTHER TRAVEL	5,000.00		(1,000.00)		4,000.00		1,510.00		0.00		2,490.00	
ASSOC DUES & MEMBERSHIPS/STAF	16,200.00		(1,700.00)		14,500.00		14,251.00		0.00		249.00	
PHYSICAL ED RELATED EXP	2,000.00		(1,822.00)		178.00		178.00		0.00		0.00	
FIELD TRIPS	3,200.00		(2,000.00)		1,200.00		740.50		235.00		224.50	
WORKSHOP RELATED COSTS	250.00		0.00		250.00		0.00		0.00		250.00	

TECH VALLEY HIGH SCHOOL
CONSOLIDATED BUDGET STATUS REPORT

12/31/21

Description	Initial Budget		Adjustments		Current Budget		Year-to-Date Expenditures		Encumbrances Outstanding		Unencumbered Balance	
TRANSPORTATION	10,500.00		(7,000.00)		3,500.00		549.81		2,950.19		0.00	
PRINTING & COPYING	1,000.00		0.00		1,000.00		68.35		931.65		0.00	
OTHER MISC EXPENSE	25,292.00		0.00		25,292.00		19,482.99		2,095.51		3,713.50	
400 Subtotal Contractual & Other	131,268.00		78,821.00		210,089.00		142,562.94		55,372.82		12,153.24	

TECH VALLEY HIGH SCHOOL CONSOLIDATED BUDGET STATUS REPORT

12/31/21

Description	Initial Budget	Adjustments	Current Budget	Year-to-Date Expenditures	Encumbrances Outstanding	Unencumbered Balance
440 CONTRACTED PROFESSIONAL SERVICES						
ACCOUNTANTS & AUDITORS	7,865.00	7,865.00	15,730.00	7,865.00	7,865.00	0.00
440 Subtotal Contracted	7,865.00	7,865.00	15,730.00	7,865.00	7,865.00	0.00
470 Rental of Facilities						
CONTRIBUTED RENT	0.00	695,951.00	695,951.00	294,619.28	0.00	401,331.72
RENTAL OF FACILITY	86,700.00	0.00	86,700.00	47,843.58	34,453.48	4,402.94
470 Subtotal Services From Rental of	86,700.00	695,951.00	782,651.00	342,462.86	34,453.48	405,734.66
490 SERVICES FROM SCH DIST & BOCES						
490 Subtotal Services From Sch Dist	148,591.00	(96,163.00)	52,428.00	12,775.08	4,000.93	35,651.99
800 EMPLOYEE BENEFITS						
EMPLOYEE BENEFITS	6,250.00	0.00	6,250.00	0.00	0.00	6,250.00
TEACHERS RETIREMENT	138,697.13	18,155.42	156,852.55	69,930.18	69,249.39	17,672.98
EMPLOYEE RETIREMENT	15,626.00	1,525.00	17,151.00	8,038.08	9,110.35	2.57
SOCIAL SECURITY	114,059.25	0.00	114,059.25	56,851.05	57,332.63	875.57
HEALTH INSURANCE	350,488.00	(6,347.00)	344,141.00	170,701.70	170,808.84	2,630.46
DENTAL INSURANCE	7,536.00	(142.98)	7,393.02	3,672.00	3,672.00	49.02
UNEMPLOYMENT INSURANCE	15,015.62	(10,184.00)	4,831.62	0.00	0.00	4,831.62
EMPLOYEE TUITION	4,500.00	0.00	4,500.00	1,800.00	2,700.00	0.00
DISABILITY INSURANCE	9,125.25	(5,100.00)	4,025.25	1,522.56	1,522.56	980.13
800 Subtotal Employee Benefits	661,297.25	(2,093.56)	659,203.69	311,515.57	314,395.77	33,292.35
CURRENT EXPENDITURES BUDGET	2,671,722.25	764,066.00	3,435,788.25	1,663,524.19	1,234,525.45	537,738.61

11/6/22
Date

W. A. W. W.
Treasurer

11/6/22
Date

W. A. W. W.
Finance Specialist II

**TECH VALLEY REGIONAL HIGH SCHOOL
EXTRA CLASSROOM ACCOUNT**

MONTH OF November 30, 2021

Cash Balance as of: October 31, 2021
Extra Classroom- Key Bank

8,798.01

TOTAL BEGINNING CASH:

\$ 8,798.01

RECEIPTS:

Extra Classroom- Key Bank

-

TOTAL RECEIPTS:

-

DISBURSEMENTS:

Extra Classroom- Key Bank

350.00

TOTAL DISBURSEMENTS:

350.00

Cash Balance as of November 30, 2021
Extra Classroom- Key Bank

8,448.01

TOTAL ENDING CASH:

\$ 8,448.01 ✓

BANK BALANCES

Balance per Key Bank Statement:

\$ 8,698.01

Less: Outstanding Checks- Key Checking

\$ (250.00)

(250.00)

Add: Deposits In Translt

\$ -

-

TOTAL

\$ 8,448.01

Verified by Deputy Treasurer

Prepared By Treasurer

**TECH VALLEY REGIONAL HIGH SCHOOL
CHECKING ACCOUNT**

MONTH OF November 30, 2021

Cash Balance as of October 31, 2021

General Fund - Key Bank	639,033.93
Special Aid Fund - Key	79,420.49
T&A Fund - Key	(348.58)
Capital Fund - Key	<u>130,641.99</u>

TOTAL BEGINNING CASH: \$ 848,749.83

RECEIPTS:

General Fund - Key	325,056.13
Special Aid Fund - Key	-
Trust & Agency Fund - Key	125,141.60
Capital Fund - Key	6.37
Interest on Investments & Savings	<u>6.37</u>

TOTAL RECEIPTS: 450,204.10

DISBURSEMENTS:

General Fund - Key	(196,351.01)
Special Aid Fund - Key	(42,955.80)
Trust & Agency Fund - Key	(125,232.06)
Capital Fund - Key	<u>-</u>

TOTAL DISBURSEMENTS: (364,538.87)

Cash Balance as of November 30, 2021

General Fund - Key	767,745.42
Special Aid Fund - Key	36,484.59
T&A Fund - Key	(437.04)
Capital Fund - Key	<u>130,641.99</u>

TOTAL ENDING CASH: \$ 934,414.96

BANK BALANCES

Balance per Key Bank Statement:

\$ 954,397.35

Less: Outstanding Checks- Key Checking

\$ (19,982.39)

(19,982.39)

Add: Deposits in Transit

\$ -

-

TOTAL

\$ -

\$ 934,414.96

Verified By:  Deputy Treasurer

Prepared By:  Treasurer

**TECH VALLEY REGIONAL HIGH SCHOOL
CHECKING ACCOUNT**

MONTH OF December 31, 2021

Cash Balance as of November 30, 2021

General Fund - Key Bank	767,745.42
Special Aid Fund - Key	38,464.69
T&A Fund - Key	(437.04)
Capital Fund - Key	<u>130,641.99</u>

TOTAL BEGINNING CASH: \$ 934,414.96

RECEIPTS:

General Fund - Key	226,419.96
Special Aid Fund - Key	-
Trust & Agency Fund - Key	124,234.01
Capital Fund - Key	-
Interest on Investments & Savings	<u>7.50</u>

TOTAL RECEIPTS: 350,681.47

DISBURSEMENTS:

General Fund - Key	(167,763.77)
Special Aid Fund - Key	(25,683.88)
Trust & Agency Fund - Key	(123,877.73)
Capital Fund - Key	<u>-</u>

TOTAL DISBURSEMENTS: (317,295.36)

Cash Balance as of December 31, 2021

General Fund - Key	826,419.11
Special Aid Fund - Key	10,800.73
T&A Fund - Key	(80.76)
Capital Fund - Key	<u>130,641.99</u>

TOTAL ENDING CASH: \$ 987,781.07

BANK BALANCES

Balance per Key Bank Statement:	\$ 971,876.91
Less: Outstanding Checks- Key Checking	\$ (4,095.84)
	<u>(4,095.84)</u>
Add: Deposits In Transit	\$ -
	<u>-</u>
TOTAL	\$ <u>987,781.07</u>


Verified By Deputy Treasurer


Prepared By Treasurer

**TECH VALLEY REGIONAL HIGH SCHOOL
EXTRA CLASSROOM ACCOUNT**

MONTH OF December 31, 2021

Cash Balance as of: November 30, 2021
Extra Classroom- Key Bank

8,448.01

TOTAL BEGINNING CASH:

\$ 8,448.01

RECEIPTS:

Extra Classroom- Key Bank

TOTAL RECEIPTS:

DISBURSEMENTS:

Extra Classroom- Key Bank

TOTAL DISBURSEMENTS:

Cash Balance as of December 31, 2021
Extra Classroom- Key Bank

8,448.01

TOTAL ENDING CASH:

\$ 8,448.01

BANK BALANCES

Balance per Key Bank Statement:

\$ 8,448.01

Less: Outstanding Checks- Key Checking

Add: Deposits In Transit

TOTAL

\$ 8,448.01


Verified by Deputy Treasurer


Prepared By Treasurer



CASH MANAGEMENT MASTER AGREEMENT

Customer: TECH VALLEY HIGH SCHOOL

TD Bank, N.A. ("Bank") provides a broad range of non-consumer cash management products and services to its customers. The customer identified above ("Customer") wishes to use, and Bank is willing to provide to Customer, those services that have been checked below:

1. TD eTreasury Services (Appendix I) ☒
2. TD ACH Origination Services (Appendix II) ☒
3. TD Wire Transfer Services (Appendix III) ☒
4. TD Sweep Services (Appendix IV)..... ☐
5. TD Positive Pay Services (Appendix V) ☒
6. TD Controlled Disbursement Services (Appendix VI)..... ☐
7. TD Lockbox Services (Appendix VII)..... ☐
8. TD Digital Express Services (Appendix VIII) ☒
9. TD Account Reconciliation Services - Full (Appendix IX)..... ☒
10. TD Account Reconciliation Services – Partial (Appendix X) ☐
11. TD Deposit Reconciliation Services (Appendix XI) ☐
12. TD Check Imaging Services (Appendix XII)..... ☐
13. TD Zero Balance Account Services (Appendix XIII)..... ☐
14. TD Currency Services (Appendix XIV)..... ☒
15. TD EscrowDirect Services (Appendix XV) ☐
16. TD Information Reporting File Transmission Services (Appendix XVI) ☐
17. TD Data Exchange Services (Appendix XVII) ☐
18. TD ACH Third Party Sender Services (Appendix XVIII)..... ☐
19. TD Image Cash Letter Services (Appendix XIX) ☐
20. TD Healthcare Remittance Management Services (Appendix XX) ☐
21. TD Data Transmission Services (Appendix XXI)..... ☒
22. TD ACH Positive Pay Services (Appendix XXII) ☒
23. TD Currency Services for Smartsafe (Appendix XXIII)..... ☐

24. TD Electronic Bill Payment Presentment & Payment Services (Appendix XXIV) ☐
25. TD Integrated Payables Processing Services (Appendix XXV)..... ☐
26. TD Electronic Lockbox (Bill Payment Aggregation) Services (Appendix XXVI) ☐
27. TD Paymode-X Services (Appendix XXVII) ☐
28. TD Integrated Receivables Services (Appendix XXVIII) ☐

The “Cash Management Service(s)” or “Service(s)” shall hereafter mean the cash management service(s) identified above and provided by Bank (and/or Bank’s third-party service providers) to Customer pursuant to this Agreement, the Appendices, including Amended Appendices, as defined below, exhibits, Setup Form(s), and any service guides or manuals made available in writing to Customer by Bank.

Agreement

This Cash Management Master Agreement is by and between Bank and Customer. This Cash Management Master Agreement shall be and is hereby incorporated by reference into and forms part of the “Contract” between the parties, the terms of which include: (1) the Request for Proposal (the “RFP”); and this Agreement. The Parties agree that any ambiguity, conflict or inconsistency in the foregoing documents that together constitute the Contract shall be resolved in the following order: (1) this Agreement; (2) and the RFP. Any and all ambiguities in the RFP documents, the RFP awards, the Agreement, or related documents shall be constructed in favor of Customer.

Bank agrees to provide to Customer and Customer agrees to use certain Cash Management Services (as defined above) offered and approved by Bank for Customer’s use. Bank and Customer agree that the Cash Management Services will be governed by the general terms and conditions of the Contract, including the rules and procedures applicable to each of the Services (collectively, the “Rules”). The Rules are contained in the Appendices to this Agreement, and are hereby incorporated in and made a part of this Agreement.

The following terms and conditions are applicable to all Cash Management Services provided to Customer hereunder.

1. Definitions. Capitalized terms used in this Agreement and in any Appendix, unless otherwise defined herein or therein, shall have the meanings set forth below:

“Access Devices” means collectively all security, identification and authentication mechanisms, including, without limitation, security codes or tokens, PINs, electronic identities or signatures, encryption keys and/or individual passwords associated with or necessary for Customer’s access to and use of any Cash Management Services.

“Account” means an Account, as such term is defined in the Account Agreement, used in connection with any Cash Management Services.

“Account Agreement” means the Business Deposit Account Agreement issued by Bank and governing Customer’s deposit relationship with Bank, as the same may be amended from time to time.

“Affiliate(s)” means, with respect to any party, any company controlled by, under the control of, or under common control with such party.

“Amended Appendix” means an amendment to an Appendix that supplements or revises, but does not revoke in its entirety, a prior Appendix for a particular Service.

“Appendix” means a description of the rules and procedures applicable to a particular Service to be provided by Bank to Customer prior to signing this Agreement and attached to this Agreement. Each such Appendix, including any Amended Appendix, is incorporated herein by reference and made a part hereof, and all references herein to Agreement shall be deemed to include all Appendices unless otherwise expressly provided. If there is any conflict between the provisions of this Agreement and any Appendix or Amended Appendix, the Appendix or Amended Appendix shall govern, but only to the extent reasonably necessary to resolve such conflict.

“Authorized Representative” means a person designated by Customer as an individual authorized to act on behalf of Customer with respect to certain matters and/or authorized to access and use the Services, as evidenced by certified copies of resolutions from Customer’s board of directors or other governing body, if any, or other certificate or evidence of authority satisfactory to Bank, including, without limitation, any Customer enrollment or Setup Form(s) completed by Customer.

“Bank Internet System” means Bank’s Internet-based electronic information delivery and transaction initiation system, as may be offered by Bank from time to time, including but not limited to Bank’s eTreasury Services.

"Bank Internet System Appendix" means the agreement issued by Bank prior to signing this Agreement that governs Customer's use of the Bank Internet System.

"Business Day" has the meaning given to it in the Account Agreement.

"Calendar Day" has the meaning given to it in the Account Agreement.

"Primary Account" means the Account designated in writing by Customer to which any direct Service fees due Bank may be charged in accordance with this Agreement. Unless otherwise agreed upon in writing by Bank, the address for Customer associated with the Primary Account shall be the address to which all notices and other communications concerning the Services may be sent by Bank.

"Substitute Check" has the meaning given to it in Section 3(16) of the *Check Clearing for the 21st Century Act* ("Check 21"), P.L. 108-100, 12 U.S.C. § 5002(16).

2. The Services.

2.1 Bank shall provide to Customer, subject to this Agreement and the applicable Appendix, all Cash Management Services that Customer may request in writing and that Bank may approve from time to time. Bank shall not be required to provide any Services specified in an Appendix unless Customer also provides all information reasonably required by Bank to provide to Customer the Service(s) specified therein.

2.2 Customer, through its Authorized Representative, may use the Services solely in accordance with the terms and conditions of this Agreement and the related Appendices.

2.3 With the exception of scheduled off-peak downtime periods, Bank shall make all reasonable efforts to make the Services available to Customer each Business Day.

2.4 Access to on-line or Internet-based Services may be denied for various reasons, including if invalid Access Devices are used or if the user exceeds the number of invalid attempts allowed by Bank.

2.5 Customer is authorized to use the Services only for the purposes and in the manner contemplated by this Agreement.

2.6 Customer agrees to reasonably cooperate with Bank, as Bank may reasonably request, in conjunction with the performance of the Services.

2.7 Customer agrees to comply with the Rules, as they may be amended from time to time by Bank.

2.8 A number of Bank's Services are subject to processing cut-off times on a Business Day.

Customer can obtain information on Bank's current cut-off time(s) for Service(s) by reviewing the relevant Service's Setup Form(s), as applicable, or by calling Treasury Management Services Support at 1-866-475-7262, or by contacting Customer's Treasury Management Services Representative. Instructions received after a cut-off time or on a day other than a Business Day will generally be deemed received as of the next Business Day.

2.9 Except for the Service Fees (as further defined in Section 4.2 of this Agreement) and scope of included Services applicable to the Term of the Contract as further described in Section 14 of this Agreement, Bank may make changes to this Agreement and any Appendix at any time by providing notice to Customer in accordance with the terms of this Agreement or as may be required by applicable law. Notwithstanding anything to the contrary herein, any Appendix that provides for an alternative form and method for making changes to such Appendix and for providing notice of the same shall govern for that Service. Further, notwithstanding anything to the contrary in the Contract, if Bank believes immediate action is necessary for the security of Bank or Customer funds, Bank may immediately initiate changes to any security procedures associated with the Services and provide prompt subsequent notice thereof to Customer.

2.10 In connection with this Agreement and the Services, Customer agrees that it shall present, and Bank shall have a duty to process, only Substitute Checks that are created by financial institutions; provided, however, that this limitation shall not apply to Substitute Checks created with data from Customer pursuant to any Appendix for Services involving the creation of electronic check images using check conversion technology.

3. Covenants, Representations and Warranties.

3.1 Customer represents and warrants that the individual(s) executing this Agreement and any other agreements or documents associated with the Services has/have been authorized by all necessary Customer action to do so, to issue such instructions as may be necessary to carry out the purposes and intent of this Agreement and to enable Customer to receive each selected Service. Each Authorized Representative whom Customer permits to access and use the Services is duly authorized by all necessary action on the part of Customer to (i) access the Account(s) and use the Services; (ii) access any information related to any Account(s) to which the Authorized Representative has access; and (iii) engage in any transaction relating to any Account(s) to which the Authorized Representative has access.

3.2 Bank may unconditionally rely on the validity and accuracy of any communication or transaction made, or purported to be made, by an Authorized Representative and in accordance with the terms of this Agreement.

3.3 Customer shall take all reasonable measures and exercise all reasonable precautions to prevent

the unauthorized disclosure or use of all Access Devices associated with or necessary for Customer's use of the Services.

3.4 Customer is not a "consumer" as such term is defined in the regulations promulgated pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., nor a legal representative of a "consumer."

3.5 Customer shall use the Services only for its own lawful business purposes. Customer shall not use the Services for or on behalf of any third party, except as may otherwise be approved by Bank in its sole and exclusive discretion, and as further described in Section 33. Customer shall take all reasonable measures and exercise reasonable precautions to ensure that Customer's officers, employees and Authorized Representatives do not use the Services for personal, family or household purposes, or for any other purpose not contemplated by this Agreement.

3.6 Customer agrees not to use or attempt to use the Services (a) to engage in any illegal purpose or activity or to violate any applicable law, rule or regulation, (b) to breach any contract or agreement by which Customer is bound, or (c) to engage in any Internet or online gambling transaction, whether or not gambling is legal in any applicable jurisdiction, or (d) to engage in any transaction or activity that is not specifically authorized and permitted by this Agreement. Customer acknowledges and agrees that Bank has no obligation to monitor Customer's use of the Services for transactions and activity that is impermissible or prohibited under the terms of this Agreement; provided, however, that Bank reserves the right to decline to execute any transaction or activity that Bank believes violates the terms of this Agreement.

3.7 Customer and Bank shall comply with (i) all applicable federal, state and local laws, regulations, rules and orders; (ii) the Account Agreement; (iii) all applicable National Automated Clearing House Association ("NACHA") rules, regulations, and policies; (iv) the Uniform Commercial Code; (v) Office of Foreign Asset Control ("OFAC") requirements; and (vi) all applicable laws, regulations and orders administered by the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") (collectively (i) through (vi), "Compliance Laws").

3.8 Bank represents and warrants that: (i) it has the authority to enter into this Agreement and it shall be bound by the terms herein; (ii) the execution, performance and delivery of any term of this Agreement or any Appendix does not infringe upon the legal rights of another individual or entity and does not create a default under any other agreement, contract or obligation of Bank; (iii) it will use due care in providing Services in a professional and workmanlike manner; (iv) it will use reasonable efforts to prevent the Services from containing known viruses, worms, Trojan horses, keystroke loggers, rootkits, spyware, dishonest adware, malware, ransomware, crimeware or other harmful, malicious or unwanted software code, files, scripts, agents or programs; (v) it is the valid owner of the Services (including any documentation, updates, subscriptions,

replacements, enhancements, improvements, or modifications thereof); (vi) the Services or any part thereof or any intended use thereof by Customer do not and will not infringe the intellectual property or other rights of any third party, including, without limitation, any patent, copyright, trade secret or other proprietary right of any third party; (vii) it will deliver the Services free from claims of any third party for infringement, including without limitation, of patents, trademarks and copyrights, improper use of intellectual property, or misappropriation of trade secrets; (viii) it maintains adequate cybersecurity systems, backup, and other protocols, policies, and procedures that are in accordance with applicable federal and state law and industry standards to protect the security of Customer's confidential information and prevent and guard against a hack or data breach, including without limitation, maintaining physical, technical, administrative, and operational controls and risk monitoring processes, as well as conducting periodic self-assessments of the security of the Services and its processes and practices with regard to the security of the Services; and (ix) it shall not collect, process, store, maintain, or transfer Customer's personally identifiable information outside of the United States and if Bank collects, processes, stores, maintains, or transfers Customer's personally identifiable information outside of the United States, Bank assumes full responsibility for compliance with foreign data privacy laws and full liability for any non-compliance with foreign data privacy laws.

4. Account Agreement; Service Fees.

4.1 Bank and Customer agree that any Account established by Customer in connection with Services offered by Bank shall be governed by the Account Agreement, including one or more fee schedules issued by Bank for the Account. If there is any conflict between the terms and provisions of this Agreement and the Account Agreement, the terms and provisions of this Agreement shall govern, but only to the extent reasonably necessary to resolve such conflict.

4.2 During the Term of the Agreement, as described in Section 14, Customer agrees to compensate Bank for all Accounts and Services that Bank provides pursuant to this Agreement, any Appendices, and in accordance with the Proposal (the "Service Fees"). Any fees and charges associated with Accounts or Services that are not specified in the Contract shall be governed by Bank's standard schedule of fees and charges applicable to Accounts or Services generally. By signing below, Customer acknowledges receipt of the Account Agreement and acceptance of the Service Fees, and agrees to be bound by their terms.

4.3 Customer authorizes Bank to charge the Primary Account for all applicable charges and fees to the extent that such charges and fees are not offset by earnings credits or other allowances for Customer's Account(s). If the balance of available funds in the Primary Account is not sufficient to cover such fees, Bank may charge such fees to any other deposit Account maintained on Bank's records in Customer's name. Customer also agrees to pay all sales, use

or other taxes (other than taxes based upon Bank's gross receipts, net income, or assets) that may be applicable to the Services provided by Bank hereunder.

4.4 During the Term of this Agreement, as described in Section 14, Bank may not amend Service Fee(s) associated with those Services provided by Bank in accordance with the Contract, unless by mutual written agreement of the parties. Bank acknowledges and agrees that the fees reflected in the Proposal, shall control and be in effect for the Term of this Agreement. Notwithstanding the foregoing, Bank may charge or amend Service Fee(s) associated with new or additional Services that Customer may request that are not included in the Services under the Contract.

5. **Customer Information.** Customer agrees to provide to Bank, before Bank begins providing any Services to Customer, any and all information that Bank requests in writing required to comply with applicable law and Bank's policies and procedures relating to customer identification and authority. Such information may include, without limitation, official certificates of customer existence, copies of Customer formation agreements, business resolutions or equivalent documents, in a form acceptable to Bank authorizing Customer to enter into this Agreement and to receive Services from Bank pursuant hereto, and designating certain individuals as Customer's Authorized Representatives.

6. Software.

6.1 Bank may supply Customer with certain software owned by or licensed to Bank to be used by Customer in connection with the Services ("Software"). Customer agrees that all such Software is and shall remain the sole property of Bank and/or the vendor of such Software. Customer agrees to comply with all of the terms and conditions of all license and other agreements which are provided to Customer in writing by Bank and/or the Software vendor and/or which govern Customer's use of Software associated with the Services. Unless otherwise agreed in writing between Bank and Customer, Customer shall be responsible for the payment of all costs of installation of any Software provided to Customer in connection with the Services, as well as for selection, installation, maintenance and repair of all hardware required on Customer's premises for the successful operation of the Software.

6.2 Except as otherwise expressly prohibited or limited by applicable law, Customer shall indemnify, defend and hold harmless Bank, its successors and assigns, from and against any loss, damage or other claim or liability attributable to Customer's unauthorized distribution or disclosure of any Software provided with the Services or any other breach by Customer of any Software license. The provisions of this paragraph shall survive termination of this Agreement.

6.3 Any breach or threatened breach of this Section will cause immediate irreparable injury to Bank, and

Customer agrees that injunctive relief, including preliminary injunctive relief and specific performance, should be awarded as appropriate to remedy such breach, without limiting Bank's right to other remedies available in the case of such a breach. Bank may apply to a court for preliminary injunctive relief, permanent injunctive relief and specific performance, but such application shall not abrogate Bank's right to proceed with an action in a court of competent jurisdiction in order to resolve the underlying dispute.

7. **Computer Requirements.** For certain Cash Management Services, Customer will need to provide, at Customer's own expense, a computer or similar Internet-enabled device, software and Internet or other connections and equipment as needed to access the Services (collectively, the "Computer"). Customer's Internet or other web browser software must support a minimum 128-bit SSL encryption or other security measures as Bank may specify in writing. Customer's browser must be one that is certified and supported by Bank for optimal performance. Customer is responsible for the installation, maintenance and operation of the Computer and all related charges, including without limitation all Internet service provider, telephone and other similar charges incurred in connecting to the Services. Customer is responsible for installing and maintaining appropriate virus protection software on Customer's Computer. Bank recommends that Customer routinely scan the Computer using reliable virus protection products, and to remove any viruses found using such products. Bank is not responsible for any errors or failures caused by any malfunction of the Computer. Bank is not responsible for any Computer virus or related problems that may be associated with access to or use of the Services, any Software, the Computer or other Internet access, including but not limited to any virus, Trojan horse, worm, keystroke logger, rootkit, spyware, dishonest adware, crimeware or other malicious or unwanted software or related problems that may be associated with access to or use of the Services, any Software or the Computer. Bank also is not responsible for any losses or delays in transmission of information Customer provides to Bank or otherwise arising out of or incurred in connection with the use of any Internet or other service provider providing Customer's connection to the Internet or any browser software. From time to time, Bank may require that Customer upgrade or install software to the Computer to ensure the proper operation of the Services. Customer agrees to promptly load any such upgrades or additional installations upon Bank's notice to Customer.

8. Bank Third Parties.

8.1 Customer acknowledges that certain third parties, agents or independent service providers (hereinafter "Third Parties") may, from time to time, provide services ("Third Party Services") to Bank in connection with Bank's provision of the Services to Customer and that accordingly, Bank's ability to provide the Services hereunder may be contingent upon the continuing availability of certain services from such Third Parties. Third Party Services may involve the processing and/or transmission of Customer's data, instructions (oral or written) and funds. In addition, Customer agrees that Bank

may disclose Customer's financial information to such Third Parties (i) where it is necessary to provide the Services requested; (ii) in order to comply with laws, government agency rules or orders, court orders, subpoenas or other legal process or in order to give information to any government agency or official having legal authority to request such information; or (iii) when Customer gives its written permission. Bank shall enter into appropriate agreements with any such Third Parties requiring said Third Parties to maintain the confidentiality, privacy, and security of Customer's information in accordance with applicable laws and standard industry best practices.

8.2 Bank will be responsible for the acts and omissions of its Third Parties in the same manner as if Bank had performed that portion of the Services itself, and no claim may be brought by Customer against such Third Parties. Notwithstanding the foregoing, any claims against Bank (with respect to the acts or omissions of its Third Parties) or its Third Parties shall be subject to the limitations of liability set forth herein to the same extent as if Bank had performed that portion of the Services itself. However, Bank will not be deemed to be the agent of, or responsible for, the acts or omissions of any person (other than its Third Parties), and no such person shall be deemed Bank's agent.

9. Customer Communications; Security Procedures.

9.1 In providing the Services, Bank shall be entitled to rely upon the accuracy of all information and authorizations received from Customer or an Authorized Representative and, where applicable, the authenticity of any signatures purporting to be of Customer or an Authorized Representative. Customer agrees promptly to notify Bank of any changes to any information or authorizations provided to Bank in connection with the Services, and further agrees to promptly execute any new or additional documentation Bank reasonably deems necessary from time to time in order to continue to provide the Services to Customer.

9.2 Customer agrees that it shall be solely responsible for ensuring its compliance with any commercially reasonable security procedures established by Bank in connection with the Services, as such may be amended from time to time, and that Bank shall have no liability for any losses sustained by Customer as a result of a breach of security procedures if Bank has complied with the security procedures.

9.3 Bank shall be entitled to rely on any written list of Authorized Representatives provided to Bank by Customer until revoked or modified by Customer in writing. Customer agrees that Bank may refuse to comply with requests from any individual until Bank receives documentation reasonably satisfactory to it confirming the individual's authority. Bank shall be entitled to rely on any notice or other writing believed by it in good faith to be genuine and correct and to have been signed by an Authorized Representative. Bank may also accept verbal instructions from persons identifying themselves as an Authorized Representative, and Bank's only obligation to

verify the identity of such person as an Authorized Representative shall be to call back such person at a telephone number(s) previously provided in writing to Bank by Customer as part of the Account or Services' Setup Form(s). Bank may, but shall have no obligation to, call back an Authorized Representative other than the Authorized Representative from whom Bank purportedly received an instruction. Bank may, but shall have no obligation to, request additional confirmation, written or verbal, of an instruction received from an Authorized Representative via telephone at any time or for any reason whatsoever prior to executing the instruction. Bank may also in its discretion require the use of security codes for Authorized Representatives and/or for receiving instructions or items from Customer. Customer understands and agrees, and Customer shall advise each Authorized Representative that, Bank may, at Bank's option, record telephone conversations regarding instructions received from an Authorized Representative.

9.4 Any security procedures maintained by Bank are not intended to detect errors in the content of an instruction received from Customer or Customer's Authorized Representative. Any errors in an instruction from Customer or Customer's Authorized Representative shall be Customer's sole responsibility. Customer agrees that all security procedures described in this Agreement and applicable Appendix are commercially reasonable and that Bank may charge Customer's Account for any instruction that Bank executed in good faith and in conformity with the security procedures, whether or not the transfer is in fact authorized.

9.5 Each of Bank and Customer agrees to adopt and implement its own commercially reasonable internal policies, procedures and systems to provide security to information being transmitted and to receive, store, transmit and destroy data or information in a secure manner to prevent loss, theft or unauthorized access to data or information ("Data Breaches"). Each of Bank and Customer also agrees that it will promptly investigate any suspected Data Breaches and monitor its systems regularly for unauthorized intrusions. Each of Bank and Customer will provide timely and accurate notification to the other party of any Data Breaches affecting the other party when known or reasonably suspected by Bank or Customer and will take all reasonable measures, which may include, without limitation, determining the scope of any data or transactions impacted by any Data Breaches affecting the other party, and promptly providing to the other party all such information to the extent affecting the other party, subject to any limitation imposed on Bank or Customer by law enforcement or applicable law or regulation.

9.6 BANK'S SECURITY PROCEDURES ARE STRICTLY CONFIDENTIAL AND SHOULD BE DISCLOSED ONLY TO THOSE INDIVIDUALS WHO ARE REQUIRED TO KNOW THEM OR AS OTHERWISE PROVIDED BY LAW. IF A SECURITY PROCEDURE INVOLVES THE USE OF ACCESS DEVICES, THE CUSTOMER SHALL BE RESPONSIBLE TO SAFEGUARD THESE ACCESS DEVICES AND

MAKE THEM AVAILABLE ONLY TO DESIGNATED INDIVIDUALS. CUSTOMER HAS THE SOLE RESPONSIBILITY TO INSTRUCT THOSE INDIVIDUALS THAT THEY MUST NOT DISCLOSE OR OTHERWISE MAKE AVAILABLE TO UNAUTHORIZED PERSONS THE SECURITY PROCEDURE OR ACCESS DEVICES. CUSTOMER HAS THE SOLE RESPONSIBILITY TO ESTABLISH AND MAINTAIN ITS OWN PROCEDURES TO ASSURE THE CONFIDENTIALITY OF ANY PROTECTED ACCESS TO THE SECURITY PROCEDURE.

10. Fraud Detection / Deterrence; Positive Pay.

Bank offers certain products and services such as Positive Pay (with or without payee validation), ACH Positive Pay, and Account blocks and filters that are designed to detect and/or deter check, automated clearing house ("ACH") or other payment system fraud. While no product or service will be completely effective, Bank believes that the products and services it offers will reduce the likelihood that certain types of fraudulent items or transactions will be paid against Customer's Account. Failure to use such products or services could substantially increase the likelihood of fraud. Customer agrees that if, after being informed by Bank or after Bank otherwise makes information about such products or services available to Customer consistent with Section 27 of this Agreement, Customer declines or fails to implement and use any of these products or services, or fails to follow these and other Bank-identified or recommended precautions reasonable for Customer's particular circumstances, Customer will be precluded from asserting any claims against Bank for paying any unauthorized, altered, counterfeit or other fraudulent item that such product, service, or precaution was designed to detect or deter, and Bank will not be required to re-credit Customer's Account or otherwise have any liability for paying such items, except to the extent that Bank has failed to exercise the required standard of care under the Uniform Commercial Code.

11. Duty to Inspect. Customer is responsible for monitoring all Services provided by Bank, including each individual transaction processed by Bank, and notifying Bank of any errors or other problems within ten (10) Calendar Days (or such longer period as may be required by applicable law) after Bank has made available to Customer any report, statement or other material containing or reflecting the error, including an Account analysis statement or on-line Account access. Except to the extent otherwise required by law, failure to notify Bank of an error or problem within such time will relieve Bank of any and all liability for interest upon correction of the error or problem (and for any loss from any subsequent transaction involving the same error or problem). In the event Customer fails to report such error or problem within thirty (30) Calendar Days after Bank made available such report, statement or on-line Account access, the transaction shall be deemed to have been properly authorized and executed, and Bank shall have no liability with respect to any error or problem. Customer agrees that its sole remedy in the event of an error in implementing any selection with the Services shall be to have Bank correct the

error within a reasonable period of time after discovering or receiving notice of the error from Customer.

12. Overdrafts; Set-off. Bank may, but shall not be obligated to, complete any transaction in connection with providing the Services if there are insufficient available funds in Customer's Account(s) to complete the transaction. In the event any actions by Customer result in an overdraft in any of Customer's Accounts, including but not limited to Customer's failure to maintain sufficient balances in any of Customer's Accounts, Customer shall be responsible for repaying the overdraft immediately, without notice or demand. Bank has the right, in addition to all other rights and remedies available to it, to set off the unpaid balance of any amount owed it in connection with the Services against any debt owing to Customer by Bank, including, without limitation, any obligation under a repurchase agreement or any funds held at any time by Bank, whether collected or in the process of collection, or in any other Account maintained by Customer at, or evidenced by any certificate of deposit issued by, Bank. Except as otherwise expressly prohibited or limited by law, if any of Customer's Accounts become overdrawn, under-funded or for any reason contain a negative balance, then Bank shall have the right of set-off against all of Customer's Accounts and other property or deposit Accounts maintained at Bank, and Bank shall have the right to enforce its interests in collateral held by it to secure debts of Customer to Bank arising from notes or other indebtedness now or hereafter owing or existing under this Agreement, whether or not matured or liquidated.

13. Transaction Limits.

13.1 In the event that providing the Services to Customer results in unacceptable credit exposure or other risk to Bank, or will cause Bank to violate any law, regulation, rule or order to which it is subject, Bank may, in Bank's sole and exclusive discretion, without prior notice, limit Customer's transaction volume or dollar amount and refuse to execute transactions that exceed any such limit, or Bank may terminate any Service then being provided to Customer. Bank will provide notice of such limits to Customer in accordance with the terms of this Agreement. Bank will communicate such limits to Customer as described in Section 13 to the extent that and in the same form and manner as Bank provides to all or substantially all of its Cash Management Services customers.

13.2 Customer shall, upon request by Bank from time to time, provide Bank with such financial information and statements and such other documentation as Bank reasonably determines to be necessary or appropriate showing Customer's financial condition, assets, liabilities, stockholder's equity, current income and surplus, and such other information regarding the financial condition of Customer as Bank may reasonably request to enable Bank to evaluate its exposure or risk. Any limits established by Bank hereunder shall be made in Bank's sole discretion and shall be communicated promptly to Customer.

14. Term and Termination.

14.1 This Agreement shall be effective when (i) signed by an Authorized Representative of Customer and Bank, and (ii) Customer delivers to Bank all documents and information, including any Setup Form(s) and electronic data, reasonably required by Bank prior to commencing to provide the Services or otherwise in accordance with the Contract, and shall terminate three (3) years after the date set forth on the signature page of this Agreement (the "Initial Term"). The parties may renew this Agreement by mutual written agreement of Customer and Bank for three (3) additional and consecutive one (1) year periods (the "Renewal Term(s)"). Bank will determine the adequacy of such documentation and information in its sole discretion and may refuse to provide the Services to Customer until adequate documentation and information are provided.

14.2 This Agreement shall continue in effect as described in Section 14.1, unless and until terminated by either party with thirty (30) Calendar Days' prior written notice to the other. Either party may terminate an Appendix in accordance with the provisions of this Section without terminating either this Agreement or any other Appendix. Upon termination of this Agreement or any Appendix, Customer shall, at its expense, return to Bank, in the same condition as when delivered to Customer, normal wear and tear excepted, all property belonging to Bank and all proprietary material delivered to Customer in connection with the terminated Service(s).

14.3 If an Appendix is terminated in accordance with this Agreement, Customer must contact Treasury Management Services Support for instructions regarding the cancellation of all future dated payments and transfers. Bank may continue to make payments and transfers and to perform other Services that Customer has previously authorized or may subsequently authorize; however, Bank is not under any obligation to do so. Bank will not be liable if it chooses to make any payment or transfer or to perform any other Services that Customer has previously authorized or subsequently authorizes after an Appendix had terminated.

14.4 Notwithstanding the foregoing, Bank may, without prior notice, terminate this Agreement and/or terminate or suspend any Service(s) provided to Customer pursuant hereto (i) if Customer or Bank closes any Account established in connection with the Service(s) that is necessary for the ongoing use of the Service(s) or necessary for Bank to charge Service Fees, including, but not limited to, closure of the Primary Account, (ii) if Bank determines that Customer has failed to maintain a financial condition deemed reasonably satisfactory to Bank to minimize any credit or other risks to Bank in providing Services to Customer, including the commencement of a voluntary or involuntary proceeding under the United States Bankruptcy Code or other statute or regulation relating to bankruptcy or relief of debtors, (iii) in the event of a material breach, default in the performance or observance of any term, or material breach of any representation or warranty by Customer, (iv) in the event of default by Customer in the payment of any sum owed by Customer to Bank hereunder or under any note or other agreement, as may be defined

therein, (v) if there has been a seizure, attachment, or garnishment of Customer's Accounts, assets or properties, (vi) if Bank believes immediate action is necessary for the security of Bank or Customer funds or (vii) if Bank reasonably believes that the continued provision of Services in accordance with the terms of this Agreement or any Appendix would violate federal, state or local laws or regulations, or would subject Bank to unacceptable risk of loss. In the event of any termination hereunder, all fees due Bank under this Agreement as of the time of termination shall become immediately due and payable. Notwithstanding any termination, this Agreement shall remain in full force and effect with respect to all transactions initiated prior to such termination.

15. Limitation of Liability; Disclaimer of Warranties.

15.1 Customer acknowledges that Bank's fees and charges for the Services are very small in relation to the amounts of transfers initiated through the Services and, as a result, Bank's willingness to provide the Services is based on the limitations and allocations of liability contained in this Agreement. Unless expressly prohibited or otherwise restricted by applicable law, the liability of Bank in connection with the Services will be limited to actual damages sustained by Customer and only to the extent such damages are a direct result of Bank's gross negligence, willful misconduct, or bad faith. In no event shall Bank be liable for any consequential, special, incidental, indirect, punitive or similar loss or damage that Customer may suffer or incur in connection with the Services, including, without limitation, attorneys' fees, lost earnings or profits and loss or damage from subsequent wrongful dishonor resulting from Bank's acts, regardless of whether the likelihood of such loss or damage was known by Bank and regardless of the basis, theory or nature of the action on which a claim is asserted. Unless expressly prohibited by or otherwise restricted by applicable law, and without limiting the foregoing, except for gross negligence, willful misconduct, or fraud, breaches of the confidentiality and data security provisions hereunder, or violations of law or regulation, Bank's aggregate liability to Customer for all losses, damages, and expenses incurred in connection with any single claim shall not exceed an amount equal to the monthly billing paid by, charged to or otherwise assessed against Customer for Services over the twelve (12) month-period immediately preceding the date on which the damage or injury giving rise to such claim is alleged to have occurred or such fewer number of preceding months as this Agreement has been in effect. Notwithstanding any of the foregoing, for transactions which are subject to Article 4A of the UCC, Bank shall be liable for such damages as may be required or provided under Article 4A or the Fedwire Regulations, as applicable, except as otherwise agreed in this Agreement. This Agreement is only between Bank and Customer, and Bank shall have no liability hereunder to any third party.

15.2 Except as otherwise expressly provided in Section 8 of this Agreement, Bank shall not be liable for any loss, damage or injury caused by any act or omission of any third party; for any charges imposed by any third party;

or for any loss, damage or injury caused by any failure of the hardware or software utilized by a third party to provide Services to Customer.

15.3 Bank shall not be liable or responsible for damages incurred as a result of data supplied by Customer that is inaccurate, incomplete, not current, or lost in transmission. It is understood that Bank assumes no liability or responsibility for the inaccuracy, incompleteness or incorrectness of data as a result of such data having been supplied to Customer through data transmission.

15.4 Bank is not liable for failing to act sooner than required by any Appendix or applicable law. Bank also has no liability for failing to take action if Bank had discretion not to act.

15.5 Bank shall not be responsible for Customer's acts or omissions (including, without limitation, the amount, accuracy, timeliness of transmittal or due authorization of any entry, funds transfer order, or other instruction received from Customer) or the acts or omissions of any other person, including, without limitation, any Automated Clearing House processor, any Federal Reserve Bank, any financial institution or bank, any transmission or communication facility, any receiver or receiving depository financial institution, including, without limitation, the return of an entry or rejection of a funds transfer order by such receiver or receiving depository financial institutions, and no such person shall be deemed Bank's agent. Bank shall be excused from failing to transmit or delay in transmitting an entry or funds transfer order if such transmittal would result in Bank's having exceeded any limitation upon its intra-day net funds position established pursuant to Federal Reserve guidelines or otherwise violating any provision of any risk control program of the Federal Reserve or any rule or regulation of any other U.S. governmental regulatory authority. In no event shall Bank be liable for any damages resulting from Bank's action or inaction which is consistent with regulations issued by the Board of Governors of the Federal Reserve System, operating circulars issued by a Federal Reserve Bank or general banking customs and usage. To the extent required by applicable laws, Bank will compensate Customer for loss of interest on funds as a direct result of Bank's failure to comply with such laws in executing electronic transfers of funds, if such failure was within Bank's control. Bank shall not be liable for Customer's attorney's fees in connection with any such claim.

15.6 EXCEPT AS OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER EXPRESSLY AGREES THAT USE OF THE SERVICES IS AT CUSTOMER'S SOLE RISK, AND THE SERVICE IS PROVIDED "AS IS," AND BANK AND ITS SERVICE PROVIDERS AND AGENTS DO NOT MAKE, AND EXPRESSLY DISCLAIM ANY, WARRANTIES, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE SERVICES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, OR THAT THE SERVICES WILL

BE UNINTERRUPTED OR ERROR FREE, WITHOUT BREACHES OF SECURITY OR WITHOUT DELAYS. IN THOSE STATES THAT DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE LIABILITY OF BANK AND ITS SERVICE PROVIDERS AND AGENTS IS LIMITED TO THE FULLEST POSSIBLE EXTENT PERMITTED BY LAW.

15.7 The provisions of this Section 15 shall survive termination of this Agreement.

16. Indemnification.

16.1 Except as otherwise expressly prohibited or limited by law, Customer shall indemnify and hold Bank harmless from any and all liabilities, losses, damages, costs, and expenses of any kind (including, without limitation, the reasonable fees and disbursements of counsel in connection with any investigative, administrative or judicial proceedings, whether or not Bank shall be designated a party thereto) which may be incurred by Bank due to any claim or action by any person, entity or other third-party against Bank to the extent such claim or action relates to or arises out of:

(i) any claim of any person that (a) Bank is responsible for any act or omission of Customer or (b) a Customer payment order contravenes or compromises the rights, title or interest of any third party, or contravenes any law, rule, regulation, ordinance, court order or other mandate or prohibition with the force or effect of law;

(ii) any failure by Customer to observe and perform properly all of its obligations hereunder or any wrongful act of Customer or any of its Affiliates;

(iii) any breach by Customer of any of its warranties, representations or agreements;

(iv) any action taken by Bank in reasonable reliance upon information provided to Bank by Customer or any Affiliate or subsidiary of Customer; and

(v) any legal action that Bank responds to or initiates, including any interpleader action Bank commences, involving Customer or Customer's Account(s), including without limitation, any state or federal legal process, writ of attachment, execution, garnishment, tax levy or subpoena.

16.2 The provisions of this Section 16 shall survive termination of this Agreement.

17. RESERVED.

18. **Force Majeure.** Neither party shall bear responsibility for non-performance of this Agreement to the extent that such non-performance is caused by an event beyond that party's control, including, but not necessarily limited to, fire, casualty, breakdown in equipment or failure of telecommunications or data processing services, lockout,

strike, unavoidable accident, act of God, riot, war or the enactment, issuance or operation of any adverse governmental law, ruling, regulation, order or decree, or an emergency that prevents Bank or Customer from operating normally.

19. Documentation. The parties acknowledge and agree that all documents evidencing, relating to or arising from the parties' relationship may be scanned or otherwise imaged and electronically stored and the originals (including manually signed originals) destroyed. The parties agree to treat such imaged documents as original documents and further agree that such reproductions and copies may be used and introduced as evidence at any legal proceedings including, without limitation, trials and arbitrations, relating to or arising under this Agreement.

20. Entire Agreement. Bank and Customer acknowledge and agree that the Contract and any amendments hereto, all other documents incorporated by reference therein, constitute the complete and exclusive statement of the agreement between them with respect to the Services, and supersede any prior oral or written understandings, representations, and agreements between the parties relating to the Services.

21. Amendments. Except for the Service Fees (as further defined in Section 4.2 of this Agreement) and scope of included Services applicable to the Term of the Contract, Bank may, at any time, amend this Agreement, the Services or Appendices in its sole discretion and from time to time. Except as expressly provided otherwise in this Agreement, any such changes generally will be effective as provided in the notice to Customer as described below. Customer will be deemed to accept any such changes if Customer accesses or uses any of the Services after the date on which the change becomes effective. Customer will remain obligated under this Agreement and any Appendices, including without limitation, being obligated to pay all amounts owing thereunder, even if Bank amends this Agreement or any Appendices. Notwithstanding anything to the contrary in this Agreement, in any Appendix or the Contract, if Bank believes immediate action is necessary for the security of Bank or Customer funds, Bank may immediately initiate changes to any security procedures and provide prompt subsequent notice thereof to Customer. As set forth in Section 14.2, Customer may terminate this Agreement or any Appendix upon its receipt of any notice of change that is not acceptable to Customer.

22. Severability. If any provision of this Agreement shall be determined by a court of competent jurisdiction to be unenforceable as written, that provision shall be interpreted so as to achieve, to the extent permitted by applicable law, the purposes intended by the original provision, and the remaining provisions of this Agreement shall continue intact. In the event that any statute, regulation or government policy to which Bank is subject and that governs or affects the transactions contemplated by this Agreement, would invalidate or modify any portion of this Agreement, then this Agreement or any part thereof shall be deemed amended to the extent necessary to comply with

such statute, regulation or policy, and Bank shall incur no liability to Customer as a result of Bank's compliance with such statute, regulation or policy.

23. Assignment and Delegation. Each of Bank and Customer may not sell, convey, assign, delegate or otherwise transfer this Agreement or its rights or responsibilities under this Agreement without the other party's prior written consent, which consent may be granted or withheld in such party's sole discretion.

24. Successors. This Agreement shall be binding upon and inure to the benefit of the parties and their successors and permitted assigns.

25. Non-Waiver, Cumulative Rights. No deviation from any of the terms and conditions set forth or incorporated in this Agreement shall constitute a waiver of any right or duty of either party, and the failure of either party to exercise any of its rights hereunder on any occasion shall not be deemed to be a waiver of such rights on any future occasion.

26. Governing Law. Any claim, controversy or dispute arising under or related to this Agreement shall be governed by and interpreted in accordance with federal law and, to the extent not preempted or inconsistent therewith, by the laws of the State of New Jersey.

27. Notices.

27.1 Except as otherwise expressly provided in this Agreement, all notices that are required or permitted to be given by Customer (including all documents incorporated herein by reference) shall be sent by first class mail, postage prepaid, and addressed to Bank at the address provided to Customer in writing for that purpose. All such notices shall be effective upon receipt.

27.2 Customer authorizes Bank to, and Customer agrees that Bank may, send any notice or communication that Bank is required or permitted to give to Customer under this Agreement, including but not limited to notice of any change to the Services, this Agreement or any Appendix, to Customer's business mailing address or Customer's business e-mail address as it appears on Bank's records, or electronically by posting the notice on Bank's website, on an Account statement or via facsimile, and that any such notice or communication will be effective and deemed delivered when provided to Customer in such a manner. Customer agrees to notify Bank promptly about any change in Customer's business mailing or Customer's business e-mail address and acknowledges and agrees that no such change will be effective until Bank has had a reasonable opportunity to act upon such notice. Customer agrees that Bank may consider any such notice or communication as being given to all Account owners when such notice or communication is given to any one Account owner.

28. Jury Trial Waiver. BANK AND CUSTOMER EACH AGREE THAT NEITHER BANK NOR

CUSTOMER SHALL (I) SEEK A JURY TRIAL IN ANY LAWSUIT, PROCEEDING, COUNTERCLAIM, OR ANY OTHER ACTION BASED UPON, OR ARISING OUT OF, THIS AGREEMENT OR ANY ACCOUNT OR THE DEALINGS OF THE RELATIONSHIP BETWEEN BANK AND CUSTOMER, OR (II) SEEK TO CONSOLIDATE ANY SUCH ACTION WITH ANOTHER IN WHICH A JURY TRIAL CANNOT BE OR HAS NOT BEEN WAIVED. THE PROVISIONS OF THIS SECTION SHALL BE SUBJECT TO NO EXCEPTIONS. NEITHER BANK NOR CUSTOMER HAS AGREED WITH OR REPRESENTED TO THE OTHER THAT THE PROVISIONS OF THIS SECTION WILL NOT BE FULLY ENFORCED IN ALL INSTANCES. BANK AND CUSTOMER EACH ACKNOWLEDGE THAT THIS WAIVER HAS BEEN KNOWINGLY AND VOLUNTARILY MADE. The provisions of this Section 28 shall survive termination of this Agreement.

29. Beneficiaries. This Agreement is for the benefit only of the undersigned parties hereto and is not intended to and shall not be construed as granting any rights to or otherwise benefiting any other person.

30. Recording of Communications. Customer and Bank agree that all telephone conversations or data transmissions between them or their agents made in connection with this Agreement and related to the Services may be recorded and retained by either party by use of any reasonable means, except as otherwise expressly prohibited or limited by applicable law.

31. Facsimile Signature. The parties acknowledge and agree that this Agreement and any Appendix or Amended Appendices may be executed and delivered by facsimile, and that a facsimile signature shall be treated as and have the same force and effect as an original signature. Notwithstanding the foregoing, Bank may, in its sole and exclusive discretion, also require Customer to deliver this Agreement and any Appendix or Amended Appendices with an original signature for its records.

32. Relationship. Customer and Bank are not, and Customer and Bank's licensors are not, partners, joint venturers or agents of each other as a result of this Agreement.

33. Third-Party Service Provider Activities.

33.1 Customer As a Third-Party Service Provider. Subject to Bank's prior approval and in its sole and exclusive discretion, Customer may be permitted to use one or more of the Services provided hereunder on behalf of and in conjunction with Accounts that belong to Customer's clients, who may or may not otherwise be customers of Bank, as well as on Customer's own behalf (hereinafter, when acting in such capacity, referred to as "Customer As Service Provider"). Customer shall execute any such other agreement(s) or documents as deemed necessary or appropriate by Bank prior to the initiation or continuation by Customer of any Services in such capacity. Customer agrees that Bank retains the right to reject any request by Customer

to engage in Customer As Service Provider activities as well as any transactions initiated by Customer in such capacity, in Bank's sole discretion. In the event Bank approves Customer's use of the Services in the capacity of Customer As Service Provider, then the following shall also apply:

(a) Customer represents and warrants to Bank that each Customer client has given Customer authority to access and conduct transactions with respect to its Accounts through use of any of the Services to the same extent as if Customer owned them, including in the capacity of a "third party service provider;"

(b) each reference to "Customer" in the Agreement will be deemed to be a collective reference to Customer and each Customer client whose Accounts are included in Bank's implementation of Customer's set-up for the Services;

(c) all of the provisions set forth in the Agreement will apply to Customer client's Account(s) as if Customer owned them;

(d) each person who is authorized to act on Customer's behalf with respect to a Service is also authorized to act on Customer's behalf to the same extent with respect to the Accounts of each Customer client whose Accounts are included in Bank's implementation of Customer's set-up for that Service; and

(e) Customer shall be liable for all monetary, confidentiality and other obligations to Bank under this Agreement as they relate to Customer's use of the Services for itself as well as each such Customer client. Bank may require written confirmation from each Customer client that it has authorized Customer to include its Accounts in Bank's implementation of Customer's set-up for the Services, and Customer agrees to notify Bank immediately if that authority is revoked or changed.

33.2 Customer Engaging a Third-Party Service Provider. Subject to Bank's prior approval and in its sole and exclusive discretion, Customer may appoint a third-party service provider to act as Customer's agent to use one or more of the Services (hereinafter such third-party to be referred to as "Customer's Third-Party Service Provider"). In such event, all transactions received by Bank from Customer's Third-Party Service Provider are hereby authorized by Customer. All acts and omissions of Customer's Third-Party Service Provider shall be the acts, omissions and responsibility of Customer and shall be governed by the provisions of this Agreement. Customer agrees, jointly and severally with Customer's Third-Party Service Provider, to indemnify and hold Bank harmless from any and all liabilities, losses, damages, costs and expenses of any kind (including, without limitation, the reasonable fees and disbursements of counsel in connection with any investigative, administrative or judicial proceedings, whether or not Bank shall be designated a party thereto) which may be incurred by Bank relating to or arising out of the acts or omissions of Customer's Third-Party Service Provider on behalf of Customer. Customer and Customer's

Third-Party Service Provider shall execute any such other agreement(s) or documents as deemed necessary or appropriate by Bank prior to the initiation or any continuation by Customer's Third-Party Service Provider of any Services on Customer's behalf. Notice of any termination of Customer's Third-Party Service Provider's authority to use one or more of the Services on Customer's behalf shall be given to Bank in writing. The effective date of such termination shall be ten (10) Business Days after Bank receives written notice of such termination. Customer agrees that Bank retains the right to reject any transactions initiated by Customer's Third-Party Service Provider in its sole discretion.

34. Section Headings. The section headings used in this Agreement are only meant to organize this Agreement, and do not in any way limit or define Customer's or Bank's rights or obligations.

35. Confidentiality. In further consideration of the terms of this Agreement, each party expressly covenants and agrees that, effective as of its execution of this Agreement, such party will not disclose, nor authorize its agents or attorneys to disclose, directly or indirectly, orally or in writing, spontaneously or in response to inquiries from any entity or person, the terms of this Agreement, and any other document or agreement to which reference is made herein, or any confidential or proprietary information of the other party including any personally identifiable information, except pursuant to any order, summons or other legal process issued by any state or federal court, or any state, federal, municipal or other governmental agency, or as required by applicable law, or as reasonably necessary to tax advisors, attorneys, accountants, and other professionals, or as necessary to fulfill any contractual undertakings hereunder. Each party expressly recognizes that any unauthorized disclosure of information specified herein, or any threatened disclosure, would cause irreparable injury to the other party which may not be adequately compensated by damages. Accordingly, in the event of a breach or threatened breach of the provisions of Section 35 of this Agreement by a party, The non-breaching party shall be entitled to an injunction restraining and prohibiting Customer from doing so or continuing to do so. Nothing herein shall be construed as prohibiting the non-breaching party from pursuing any other remedies available for such breach or threatened breach, including the recovery of damages. The restrictions set forth in this Section 35 shall not apply to information which (i) was, is or becomes public knowledge not in violation of this Section 35; (ii) is acquired by Customer from a third party lawfully possessing such information; or (iii) is disclosed in testimony, pleadings or papers filed by Bank or Customer in any judicial proceeding. Each party understands and agrees that this Section 35 is a material provision of this Agreement, that the other party would not have entered into this Agreement without such confidentiality obligations, and that any breach of this Section 35 shall be a material breach of this Agreement.

36. Collateral. The Bank shall enter into a third party custodian agreement (the "Third Party Custodian Agreement") with Customer providing for daily Bank

monitoring of deposit balances. The Third Party Custodian Agreement must fully collateralize all deposits not insured by the Federal Deposit Insurance Corporation ("FDIC") at a minimum of one hundred two percent (102%) of daily account balances, in strict accordance with the New York State Comptroller's guidelines and all other applicable regulations. Bank shall be responsible to ensure that Customer's requirement of continuous full collateralization is met at all times. Bank will monitor Customer's deposit balances each Business Day and Bank will maintain appropriate collateral in accordance with the New York State Comptroller's guidelines and other applicable regulations. Bank must provide Customer with FDIC insurance on all applicable deposits and investments under FDIC guidelines. Bank shall provide a collateralization statement to Customer on a monthly basis. Bank shall also provide monthly compensating balance reports showing each bank account activity, banking charges, earnings credit and associated data.

37. Advertising. Bank shall not advertise or publish without the prior written approval of Customer, the fact that Customer has entered into this Agreement or any other agreement with Bank, except to the extent necessary to comply with proper requests for information from an authorized representative of the federal, state, or local government.

38. Representations. No information derived from inspection of Customer records or reports of investigation concerning this Agreement, will in any way relieve Bank from its responsibility or from properly performing its obligations under this Agreement. Customer may have provided information as a convenience to Bank and did so without making any warranty whatsoever by Customer. Bank is responsible for making its own conclusions and interpretations from the data supplied by Customer from information available from other sources.

39. Cumulative Rights. The rights and remedies provided by this Agreement are cumulative and the use of one right or remedy by a party shall not preclude or waive the right to use any or all of the remedies available to such party.

40. Default. If Bank is in default under this Agreement or any Appendix, Customer may, in its discretion, do all things necessary to affect compliance with the laws, regulations, bylaws, directives, rules and conventions referred to in this Agreement and the RFP, and Bank shall, on demand by Customer, reimburse Customer for all costs incurred by Customer for that purpose.

41. Remedies. Bank and Customer agree that both parties have all rights, duties and remedies available, as stated in the New York Uniform Commercial Code.

42. Ethics. Bank shall not accept or offer gifts or anything of value, nor enter into any business arrangement with any employee, official or agent of Customer.

43. Non Discrimination Requirement. In accordance with Article 5 of the Executive Law of New York State (also known as the Human Rights Law) and all

other state and federal statutory and constitutional, non-discrimination provisions, Bank agrees that neither it nor its subcontractors shall by reason of race, creed, color, national origin, age, sex or disability: (a) discriminate in hiring against any person who is qualified and available to perform the work under this Agreement; or (b) discriminate against or intimidate any employee hired for the performance of work under this Agreement.

44. Patents/Copyrights/Trademarks. Bank agrees to protect Customer from claims involving infringement of patents, trademarks and/or copyrights. Bank agrees to ascertain whether the services, products, and/or software provided by Bank will cause the rightful claim of any third person by way of infringement or the like. Customer makes

no warranty that the services, products, and/or software requested by Customer and provided by Bank will not cause such a claim, and in no event shall Customer be liable to Bank for indemnifications should Bank be sued on grounds of infringement or the like. If Bank is of the opinion that an infringement or the like will result, Bank shall have notified Customer to this effect in writing within the timeframe specified in the RFP. If Customer has not received notice within the timeframe specified in the RFP and is subsequently held liable for infringement or the like, Bank will save Customer harmless. If Bank in good faith ascertains that the services, products and/or software provided by Bank will result in infringement or the like this Agreement and all Appendices shall be null and void.

IN WITNESS WHEREOF, Customer and Bank have duly caused this Agreement, including all applicable Appendices, to be executed by an Authorized Representative.

Date: 2021

TECH VALLEY HIGH SCHOOL

(Customer)

246 Tricentennial Drive

Albany, NY 12203

(Address)

By: _____

(Signature of Authorized Representative)

Print Name: _____

Title: _____

Governmental

TD BANK, N.A

By: _____

(Signature of Authorized Representative)

Print Name: _____

Title: _____



EXHIBIT TO CASH MANAGEMENT MASTER AGREEMENT:

GOVERNMENTAL ENTITY SERVICES

This Exhibit is incorporated by reference into the parties' Cash Management Master Agreement (the "Agreement") and applies to all Cash Management Services made available by Bank to Customer, as a governmental entity or unit. All capitalized terms used herein without definition shall have the meanings given to them in the Agreement. Bank and Customer agree that, notwithstanding anything to the contrary contained in the Agreement, the following terms and provisions shall apply to the Agreement:

TERMS AND CONDITIONS

1. Section 26, "Governing Law," of the Agreement is hereby deleted in its entirety and replaced with the following:

26. Governing Law. Any claim, controversy or dispute arising under or related to this Agreement shall be governed by and interpreted in accordance with the laws of the jurisdiction pursuant to which Customer was incorporated or otherwise organized, except where applicable federal law is controlling. In the event of a conflict between the provisions of this Agreement and any applicable law or regulation, this Agreement shall be deemed modified to the extent necessary to comply with such law or regulation.

2. The following new Section 35 is hereby added immediately after Section 34:

35. Additional Representations and Warranties. For purposes of this Section, "Governmental Unit" means: (A) any town, city, county or similar local governmental unit, including without limitation any school district or school administrative unit of any nature, water district, sewer district, sanitary district, housing authority, hospital district, municipal electric district or other political subdivision, agency, bureau, department or other instrumentality thereof, or similar quasi-governmental corporation or entity defined by applicable law, and (B) any state government or any agency, department, bureau, office or other instrumentality thereof.

(a) If Customer is a Governmental Unit of the type included in (A) above, Customer and the individual signing below represent, warrant and agree: (i) that this Agreement has been duly executed by the Treasurer, Finance Director, or other officer authorized by law with signatory authority to enter into banking services agreements; (ii) that this Agreement has been duly authorized and approved

by the governing body of Customer in accordance with applicable law, and, at Bank's request, as evidenced by the certification of the Secretary or other legal authority of the governing body and provided with this Agreement; (iii) that only persons authorized to disburse Customer funds from any Account will be enrolled as Authorized Users having access to wire transfer, ACH or Account transfer functions; (iv) that if this Agreement remains in effect for more than one budget year, upon request of Bank, Customer will ratify and provide evidence of the renewal of this Agreement in subsequent years; and (v) that this Agreement is the valid and binding obligation of Customer, enforceable against Customer in accordance with its terms.

(b) If Customer is a Governmental Unit of the type included in (B) above, Customer and the individual signing below represent, warrant and agree: (i) that this Agreement has been duly executed by a financial or other officer authorized by law with signatory authority to enter into banking services agreements on behalf of Customer; (ii) that this Agreement has been duly authorized by a senior or similar officer of Customer; (iii) that Customer has complied with all state laws and regulations, including any regulations or policies adopted by Customer with respect to electronic commerce in entering into and performing this Agreement and any related ACH or wire transfer service agreement; (iv) that only persons authorized to disburse Customer funds from any Account will be enrolled as Authorized Users having access to wire transfer, ACH or Account transfer functions; and (v) that this Agreement is the valid and binding obligation of Customer, enforceable against Customer in accordance with its terms.

(c) For a Customer of the type included in either (A) or (B) above, Customer and the individual signing below further represent, warrant and agree: (i) that upon Bank's request, Customer shall provide evidence of those persons authorized to disburse Customer funds as described in (a)(iii) and (b)(iv)

above; (ii) that upon Bank's request, Customer will certify its compliance with (a) or (b), as applicable, on an annual or other periodic basis; and (iii) that Customer will provide notice to Bank if any person authorized to disburse Customer funds as described in (a)(iii) and (b)(iv) is no longer so authorized or his/her position of such authority is terminated for any reason.

3. **Effectiveness.** Each of Bank and Customer agrees to all the terms and conditions of this Exhibit. The liability

of each of Bank and Customer under this Exhibit shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Exhibit shall remain in full force and effect until such time as a different or amended Exhibit is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.

Remainder of page intentionally left blank.



APPENDIX I

TD eTREASURY SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and governs Customer's use of the Bank Internet System (the "Services" or "eTreasury"). This Appendix may be referred to as the Bank Intranet System Appendix. All capitalized terms used herein without definition shall have the meanings given to them in the parties' Cash Management Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. Definitions.

"Account(s)" means, with respect to eTreasury, a checking, regular statement savings, money market deposit, certificate of deposit, investment or commercial loan or line of credit account(s) Customer maintains with Bank for business or non-consumer purposes that is designated by Customer for use with the Services, as described below.

"Account Agreement" means, in addition to the meaning contained in the parties' Cash Management Master Agreement, any and all agreements between Customer and Bank which govern Customer Accounts (as defined above) and which were provided to Customer when Customer opened its Account(s), or any other documents governing Customer's Account(s), each as may be amended from time to time.

"Administrator" or *"Account Administrator"* means Customer's employee(s) or other person(s) that Customer (or any Administrator designated by Customer) designates on the Services' Setup Form(s) (or by on-line changes to such designations as described below) as being its Authorized Representative, or as authorized to act on Customer's behalf, with respect to the Services.

"Authorized User" means any person Customer's Administrator designates as being authorized to access or use any of the Services on Customer's behalf.

"Login ID" means the electronic identification, in letters and numerals, assigned to Customer by Bank or to any additional Authorized Users designated by Customer's Account Administrator.

"Mobile Application" or *"Mobile App"* means the downloadable software application on a Mobile Device that Customer may use to perform certain electronic banking tasks in lieu of Customer's Computer.

"Mobile Device" means an eligible mobile communications device, which may include a mobile phone or a tablet.

"Payment" means a transfer of funds to or from Customer's Account(s).

2. Services.

2.1 This Appendix describes the terms and conditions under which Bank will provide Customer with access to and use of any of the electronic information delivery and transaction initiation services that Bank makes available using the Bank Internet System.

2.2 By accessing the Services via Customer's Computer with the Access Devices (as defined in the Cash Management Master Agreement), Customer may perform any or all of the Services described in this Appendix and selected for use in the Services' Setup Form(s) and that Bank has approved for Customer's use. Some of the Services described in this Appendix may also be available via Customer's Mobile Device using the Mobile App. Bank reserves the right to reject Customer's Services' Setup Form(s), schedules and other required documents and to refuse Customer access to or use of the Services for any reason and in Bank's sole discretion. Bank may, in its sole and exclusive discretion, introduce new features of the Services from time to time but is not required to notify Customer of the availability of any such new features.

2.3 By subscribing to the Services, Customer will have access to the Services' basic features, which include but may not be limited to, in Bank's sole and exclusive discretion, the following:

2.3.1 **Previous-Day Balance Reporting.** Previous-Day Balance Reporting allows Customer to review the balances and transaction history in Customer's checking, savings, money market deposit and loan Account(s) for such period of time as described in the Services' Setup Form(s). Customer may also view images of deposit tickets, deposit items, paid checks and return deposited items. This information may be viewed upon

implementation of the Services. The scope of the time periods for which transactional history and check images may be viewed (including pre-implementation periods) may vary and depend upon various factors, such as when Account(s) were opened and when the Services were first implemented and set-up.

2.3.2 Real-Time Balance Reporting. Real-Time Balance Reporting allows Customer to review current Account balance(s) and transaction activity in real-time.

2.3.3 Book Transfers. Book Transfers allows Customer to make intra-Bank fund transfers between Customer's checking, savings and loan Accounts.

2.3.3.1 General. Book Transfers may be made as one-time or recurring, same-day or in the future. Book Transfers may also be initiated from (i) one-Account-to-one-Account, (ii) one-Account-to-many-Accounts, or (iii) many-Accounts-to-one-Account. Recurring Book Transfers may utilize one of several repeating frequency options (weekly, monthly, etc.), as set forth in the Services. Book Transfer templates may be created and saved for frequently executed transfers. Pending Book Transfers and templates may be edited or deleted (cancelled) through the Services by Authorized Users at any time prior to the Business Day on which the associated transfer is scheduled to occur. Book Transfer amounts and the order in which such transfers occur are limited to the available balance in the Account(s) on the effective date of the transfer. For same-day transactions, Customer will need to have a sufficient available balance in the Account from which funds are to be transferred to cover the amount of the Book Transfer. For future or recurring Book Transfers, Customer will need to have sufficient available funds on the day the transaction is to occur. The number of Book Transfers from interest bearing checking and savings Accounts are subject to the terms of the Account Agreement and federal regulations. Book Transfers that Customer transmits by Bank's cut-off time as set forth on the Services' designated website or the Services' Setup Form(s) on a Business Day will be posted to the Account as of that Business Day; however, a request (whether a same-day funds transfer or a future-dated transfer) may not result in an immediate transfer of funds or immediate availability because of the time required to process the transaction. Customer is solely responsible for the review of the previous day's transaction report and the status of the Book Transfer request within the Services to ensure that the transaction was processed. Only Book Transfers initiated through the Services will be displayed on the Services' "Transfer" reports tab. All transfers are subject to the Account Agreement.

2.3.3.2 Future-Dated Book Transfer. In conjunction with Book Transfers, a request to transfer funds between Customer's Accounts may be initiated and approved for a future date. The future transfer date may be scheduled for such date in advance as may be permitted from time to time by Bank and as set forth within the Bank Internet System. Future-dated transfers may be scheduled as a one-time request or a recurring request in

a pre-determined amount, based on the instructions entered by Customer with the request. Future-dated Book Transfers will be initiated on the Business Day requested by Customer, not on the date Customer entered the transaction using the Services.

2.3.4 Stop Payment. Stop payments of checks drawn on Customer's Account(s) are subject to the terms and conditions of the Account Agreement. Notwithstanding anything in the Account Agreement to the contrary, Customer may use the Services to initiate stop payment orders for an individual check or a range of checks. Bank shall have no responsibility for losses resulting from any delay in Bank's receipt of stop payment orders transmitted by means of the Bank Internet System or for Customer not taking additional actions when a response message from the Bank Internet System indicates a response other than a successful confirmation. Customer must provide Bank with the **EXACT CHECK NUMBER OR RANGE OF CHECK NUMBERS**. When known, Customer should also provide the **EXACT AMOUNT OF THE CHECK**. If the check number is incorrect in any way or the amount of the check is inaccurate by one cent or more in the stop payment order, payment will not be stopped and Bank will not be responsible for resulting losses. All other information must be reasonably accurate. Requests are generally effective when successfully entered and submitted by Customer via the Services. Notwithstanding the foregoing, Customer understands that if the stop payment request comes too late for Bank to have a reasonable time to act on it prior to paying, settling for, posting or becoming accountable for the check described in the request, then Customer's stop payment request shall be of no effect. Stop payments requested using the Bank Internet System are effective for three hundred sixty-five (365) Calendar Days unless renewed before the end of the 365-day period. Customer is solely responsible for confirming the status of a stop payment order. Except as otherwise provided by Compliance Laws or the terms of the Cash Management Master Agreement, Customer shall not have the right to stop payment on or recall any electronic fund transfers or similar payment order or transfer request given hereunder after it has been transmitted to Bank. Only stop payment orders initiated or recalled through the Bank Internet System will be displayed on the Bank Internet System's Stop Payments screen. Stop payment orders that are not initiated through the Bank Internet System may also be cancelled through the Bank Internet System.

2.3.5 E-Learning. E-Learning is a self-paced, interactive educational tool available via the Services that Customer may use to learn more about the various features or modules related to the Services, as well as how to use them.

2.3.6 Customizable Dashboard. Using this feature, Customer can configure and save Account balance views, as well as command one-click access to detailed information, balance and payment reports, and high-use transaction initiation features. It is Customer's responsibility to view the "Dashboard" for Bank notices when designating another section of the Bank Internet System as the desired landing page.

2.4 In addition to the Services as described in this Appendix and/or in the Services' Setup Form(s), additional features, modules or other Cash Management Services related to eTreasury may be offered from time to time by Bank, in its sole and exclusive discretion, including but not limited to the following:

2.4.1 Wire Transfers. Wire transfers are subject to the terms and conditions of the TD Wire Transfer Services Appendix. Once approved by Bank for use by Customer, this Service allows Customer to transfer funds electronically using the Fedwire or similar funds transfer system, typically from Customer's Account(s) to other account(s) with Bank or to account(s) at other banks. Domestic or foreign wire transfers entered through the Services will be processed as set forth in the TD Wire Transfer Services Appendix.

2.4.2 ACH Originations. ACH originations are subject to the terms and conditions of the TD Automated Clearing House (ACH) Origination Appendix, the TD Third-Party Sender Services Appendix or the TD ACH Third Party Service Provider Agreement, as applicable. Once approved by Bank for use by Customer, this Service allows Customer to initiate and approve ACH transactions that Customer desires Bank to enter into the ACH network on Customer's behalf. ACH transactions entered through the Services will be processed and settled) as set forth in the TD Automated Clearing House (ACH) Origination Appendix, the TD Third-Party Sender Services Appendix or the TD ACH Third Party Service Provider Agreement, as applicable.

2.4.3 File Transfers. File transfers is a method for Customer and Bank to send and receive reports and files (including, but not limited to, ACH, Reconciliation, Lockbox, and BAI files) to each other through the Internet and are subject to the terms and conditions of applicable Appendices. Such reports and files may also be auto-generated and auto-delivered.

2.5 Mobile App.

2.5.1 The Mobile App may not be available on all types of Mobile Devices. Customer also acknowledges that the Services may not be available on Customer's Mobile Device or may have limited utility over some mobile networks, such as when roaming.

2.5.2 *Customer understands that standard data and text messaging rates charged by the telecommunications carrier providing service for Customer's Mobile Device will apply when Customer uses its Mobile Device to enroll in and use the Services.*

3. Hours of Access. Customer generally may access the Services 24 hours a day, seven (7) days a week. Customer may not be able to access some or all of the Services from time to time, however, during any special or other scheduled maintenance periods, or during emergencies, interruptions or delays due to causes beyond Bank's control.

4. Account Designation.

4.1 Customer may designate any of Customer's Accounts maintained with Bank for business or non-consumer purposes for use with the Services. Generally, the taxpayer identification number for each Account must be the same, and each Account is subject to the other conditions set forth in this Appendix, except as Bank, in its sole discretion, may otherwise permit. Bank reserves the right to deny any Account designation for use with the Services in its sole discretion.

4.2 Customer may at any time add or delete any Account that Customer has designated for use with any of the Services, or change the Services associated with any Account, by notifying Bank in writing.

5. Administrator(s) and Authorized Users.

5.1 Customer shall designate Administrator(s) with Bank as set forth in the Services' Setup Form(s). Customer is solely responsible for designating its Administrator(s).

5.2 The Administrator(s) may designate other Administrators and/or Authorized Users. Customer accepts as its sole responsibility the Administrator's designation of other Administrators and Authorized Users. Customer understands that the Administrator(s) will control, and Customer authorizes the Administrator(s) to control, access by other Administrators and Authorized Users of the Services through the issuance of Access Devices. The Administrator(s) may add, change or terminate Customer's Authorized User(s) from time to time and in his/her sole discretion. Bank does not control access by any of Customer's Authorized Users to any of the Services. If Customer designates more than one (1) Administrator, Bank recommends that Customer manage its use of the Services and its Administrators by requiring dual control to set up new Authorized Users. Bank also recommends that Customer review and assign limits for Authorized Users that create and/or approve wire transfers and ACH transactions, as established on the Services' Setup Form(s). In the event that Bank, in its sole and exclusive discretion, assists Customer in any way with the establishment, addition or general set-up of Authorized Users, Customer understands and agrees that the Administrator(s) shall remain responsible for verifying the accuracy thereof and shall otherwise control access by any of Customer's Authorized Users to any of the Services.

5.3 Customer will require each Administrator and each Authorized User to comply with all provisions of this Appendix and all other applicable agreements. Customer acknowledges and agrees that it is fully responsible for the failure of any Administrator or any Authorized User to so comply. Customer is responsible for any Payment, transfer and other use of the Services and charges incurred by any Administrator and any Authorized User, even if such Administrator or Authorized User exceeds his/her authorization. Bank recommends that Customer require its Administrator(s) to review all entitlement reports

available through the Services with respect to Customer's Authorized User(s).

5.4 Customer acknowledges and agrees that an Authorized User is not permitted to authorize other persons/entities to use its Access Devices. Notwithstanding the foregoing, if an Authorized User does authorize other persons/entities to use the Authorized User's Access Devices in any manner, such authorization will be considered by Bank as unlimited in amount and manner, and Customer is responsible for any transactions made by such persons/entities, until Customer's Administrator has deactivated the subject Authorized User's Access Devices. Bank will not be liable for and will not reimburse Customer for any losses that may occur as a result of this authorized use of an Authorized User's Access Devices.

5.5 Whenever any Authorized User leaves Customer's employ or Customer otherwise revokes the authority of any Authorized User to access or use the Services, the Administrator(s) are solely responsible for deactivating such Authorized User's Access Devices. Customer shall notify Bank in writing whenever a sole Customer Administrator leaves Customer's employ or Customer otherwise revokes a sole Administrator's authority to access or use the Services.

6. Access Devices; Security Procedures.

6.1 Upon successful enrollment, Customer can access the Services from Bank's designated website by using Customer's Computer, Mobile Device or, as may be permitted by Bank from time to time in its sole discretion and in accordance with Bank's terms and conditions for such access, using other mobile or other Internet-enabled system(s) or device(s), along with the Services' security procedures as described from time to time. A company ID assigned to Customer by Bank, a unique Login ID and an individual password will be used for log-in by Customer's Administrator(s) and Authorized User(s). The Administrator(s) and Authorized User(s) must change his or her individual password from time to time for security purposes.).

6.2 Customer acknowledges that the Administrator(s) will, and Customer authorizes the Administrator(s) to, select other Administrators and Authorized Users by issuing to any person a unique Login ID and password (subject to the additional security procedures described below). Customer further acknowledges that the Administrator(s) may, and Customer authorizes the Administrator(s) to, change or de-activate the unique Login ID and/or password from time to time and in his or her sole discretion (subject to the additional security procedures described below).

6.3 Customer acknowledges that, in addition to the above individual passwords, access to the Services includes, as part of the Access Devices, additional security procedures, including as described below:

6.3.1 **Tokens.** An additional security procedure incorporates use of a physical security device or token ("Token") for, by way of example only, initial log-in and/or certain transactional or administrative functionality. A Token may be issued to any Authorized User(s), for example, for use in initiating and/or approving ACH transactions and wire transfers, to log in to the Services, as well as with certain administrative functionality, and/or for the creation of ACH and wire templates. Physical security of each Token is Customer's sole responsibility. With the Token, each Authorized User will receive a PIN number that the Authorized User must keep in a secure place. When an Authorized User (or Administrator) leaves Customer's employ, his or her Login ID must be deleted by Customer (or by Bank upon Customer's request) and, if a Token had been issued to such Authorized User (or Administrator), Bank must be promptly notified so that Bank may deactivate such Authorized User's (or Administrator's) Token. Any additional Authorized User requiring a Token must be authorized, in writing by Customer to Bank, for Token creation or re-creation and deployment. If applicable, fees may be assessed for additional Tokens.

6.3.2 **Payment Status Alerts.** A further security procedure requires Customer to enroll in alerts for changes to payment status ("Payment Status Alerts") within the Bank Internet System. Customer must designate the Authorized User or Administrator that will receive the email alert each time a wire transfer or ACH transaction has a status of "Pending Approval" in the Bank Internet System. Bank strongly recommends that the Authorized User or Administrator to receive such Payment Status Alert is a different Authorized User or Administrator than who will approve the wire or ACH transaction.

6.3.2.1 Payment Status Alerts are not encrypted and will never include Customer's Access Devices or full Account number(s). However, Payment Status Alerts may include Customer's name and some information about Customer's Account(s). Anyone with access to Customer's email address on file with the Bank will be able to view the contents of such Payment Status Alerts. Customer agrees to test the successful receipt of the Payment Status Alerts to make sure they are not routed to the Customer's spam or other blocked mail folder. Bank is not responsible for how Customer's email system may deliver or categorize the Payment Status Alerts.

6.3.2.2 Customer acknowledges and agrees that Customer will not include full Account number(s) or other sensitive Customer or Account information in any customized subject line.

6.3.2.3 Customer understands and agrees that Customer's Payment Status Alerts may be delayed or prevented by a variety of factors. Bank will use commercially reasonable efforts to provide Payment Status Alerts in a timely manner with accurate information. Bank neither guarantees the delivery nor the accuracy of the contents of any Payment Status Alert. Customer also agrees that Bank shall not be liable for any delays, failure to deliver, or misdirected delivery of any Payment Status Alert; for any

errors in the content of an alert; or for any actions taken or not taken by Customer or any third party in reliance on a Payment Status Alert. Customer agrees that Bank is not responsible for any costs or fees incurred as a result of Payment Status Alerts sent to email addresses or phone numbers connected with mobile or similar devices.

6.3.2.4 Certain voluntary alerts are also available to the Customer as described in Section. 9.2

6.3.34 **Dual Control.** Customer further acknowledges and agrees that all wire transfers and ACH transactions initiated through the Services require “dual control” or separation of duties. With this additional security feature, one Authorized User will create, edit, cancel, delete and restore ACH batches or wire transfer orders under his/her unique Login ID, password and Token; a second *different* Authorized User with his/her own unique Login ID, password and Token will be required to approve, release or delete ACH batches or wire transfer orders. Customer acknowledges and agrees that it must notify the Bank to designate the individuals that will serve as the first Authorized User and second Authorized User and notify the Bank to request any subsequent changes to these named individuals.

6.4 Customer accepts as its sole responsibility the selection, use, protection and maintenance of confidentiality of, and access to, the Access Devices. Customer agrees to take reasonable precautions to safeguard the Access Devices and keep them confidential. Customer agrees not to reveal the Access Devices to any unauthorized person. Customer further agrees to notify Treasury Management Services Support immediately at 1-866-475-7262 if Customer believes that the confidentiality of the Access Devices has been compromised in any manner.

6.5 The Access Devices identify and authenticate Customer (including the Administrator and Authorized Users) to Bank when Customer accesses or uses the Services. Customer authorizes Bank to rely on the Access Devices to identify Customer when Customer accesses or uses any of the Services, and as signature authorization for any Payment, transfer or other use of the Services. Customer acknowledges and agrees that Bank is authorized to act on any and all communications or instructions received using the Access Devices, where such communications were provided to Bank in accordance with the security procedures and other terms as set forth in the Cash Management Master Agreement, regardless of whether the communications or instructions are authorized. Bank owns the Access Devices, and Customer may not transfer them to any other person or entity.

6.6 Customer acknowledges and agrees that the Access Devices and other security procedures applicable to Customer’s use of the Services and set forth in this Appendix, as well as such security best practices as described by Bank from time to time and made available on the Bank Internet System, are a commercially reasonable method for the purpose of verifying whether any Payment, transfer or other use of the Services was initiated by Customer. Customer also agrees that any election Customer

may make to change or waive any optional security procedures recommended by Bank is at Customer’s risk and that any loss resulting in whole or in part from such change or waiver will be Customer’s responsibility. Customer further acknowledges and agrees that the Access Devices are not intended, and that it is commercially reasonable that the Access Devices are not intended, to detect any errors relating to or arising out of a Payment, transfer or any other use of the Services.

6.7 If Customer has reason to believe that any Access Devices have been lost, stolen or used (or may be used) or that a Payment or other use of the Services has been or may be made with any Access Devices without Customer’s permission, Customer must contact its Administrator and Bank. In no event will Bank be liable for any unauthorized transaction(s) that occurs with any Access Devices, where such communications or instructions were provided to Bank in accordance with the security procedures and other terms as set forth in the Cash Management Master Agreement.

6.8 Bank may, from time to time, propose additional or enhanced security procedures to Customer. Customer understands and agrees that if it declines to use any such additional or enhanced procedures, it will be liable for any losses that would have been prevented by such procedures. Notwithstanding anything else contained in this Appendix, if Bank believes immediate action is required for the security of Bank or Customer funds, Bank may initiate additional security procedures immediately and provide prompt subsequent notice thereof to Customer.

7. **Debiting Customer’s Account(s).** Customer authorizes Bank to charge and automatically deduct the amount of any Payment from Customer’s Account(s) (or any other Account that Customer maintains with Bank, if necessary), in accordance with the Cash Management Master Agreement and the Account Agreement.

8. **Electronic Statements.**

8.1 As an eTreasury user, and subject to Bank’s approval and applicable set-up and enrollment requirements, Customer may elect to stop or resume the mailing of paper statements for eligible Accounts by requesting this feature from Bank.

8.2 Only Accounts accessible via the Services may be enrolled for electronic statement delivery. Eligible Accounts are displayed on the “Statements” page of the Services. If Customer currently receives a consolidated periodic statement that includes multiple Accounts and Customer selects electronic statement delivery, all Accounts shown on the consolidated statement will be automatically enrolled for electronic statement delivery. For joint Accounts, only one Account owner need enroll for electronic statement delivery; provided, that each Account owner must separately enroll if that Account owner wishes to receive and have access to its Account statements electronically.

8.3 Customer’s electronic statement will generally be available within 24 hours after the statement cut-off date. The statement cut-off date for Customer’s

electronic statement is the same as Customer's paper statement. Once made available as described herein, the information contained in Customer's electronic statement shall be deemed to have been delivered to Customer personally, whether actually received or not. Customer may view, print and download current statements and such period of statement history as set forth on the Bank Internet System. To view or print an electronic statement, Customer must have an appropriate version of Adobe Acrobat software installed on Customer's Computer or Mobile Device sufficient to support access to a PDF file.

8.4 At Customer's request, Bank will send Customer a paper copy of Customer's electronic statement previously delivered through the Services at any time. Bank's standard fee then in effect and charged for paper delivery of copies of Account statements will apply. A request for a paper copy does not cause a termination of the electronic statement feature. A paper copy can be obtained until the copy is no longer required to be maintained by Bank as a record for the designated Account under applicable law or regulation.

8.5 Customer may revoke consent for the electronic statement feature for Customer's Accounts at any time by contacting Customer's Relationship Manager. Electronic posting of Customer's electronic statement on the Services' site and transmission of related email notices will continue until: (i) termination of the electronic statement feature; (ii) termination of Customer's designated Accounts with Bank; or (iii) termination of this Appendix, the Cash Management Master Agreement or Customer's use of the Services.

8.6 Bank may discontinue the electronic statements feature at any time in Bank's discretion and resume mailing paper statements to Customer. Bank may also add, modify or delete any feature of the electronic statements feature in Bank's discretion. Bank will provide Customer with notice of any change or termination in the electronic statement feature in accordance with the terms of the parties' Cash Management Master Agreement.

9. Voluntary Alerts.

9.1 The Services allow Customer to choose to receive additional optional alert messages regarding Customer's Account(s), including but not limited to messages to alert Customer about high or low Account balance thresholds, debit or credit transactions cleared, and payment status for ACH and wire transactions. Bank may add new alerts from time to time, or cancel existing alerts. If Customer has opted to receive an alert that is being canceled, Bank will notify Customer in accordance with the terms of the parties' Cash Management Master Agreement. Each alert has different options available, and Customer will be asked to select from among these options upon activation of Customer's alerts service.

9.1.1 Electronic alerts will be sent to the email address Customer has provided as Customer's primary email address for the Services or via the Services' secure messaging feature. If Customer's email address changes, Customer is responsible for informing Bank of the change. Customer can also choose to have alerts sent to a secondary email address. Changes to Customer's primary and secondary email addresses will apply to all of Customer's alerts.

9.1.2 Customer understands and agrees that Customer's alerts may be delayed or prevented by a variety of factors. Bank will use commercially reasonable efforts to provide alerts in a timely manner with accurate information. Bank neither guarantees the delivery nor the accuracy of the contents of any alert. Customer also agrees that Bank shall not be liable for any delays, failure to deliver, or misdirected delivery of any alert; for any errors in the content of an alert; or for any actions taken or not taken by Customer or any third party in reliance on an alert. Customer agrees that Bank is not responsible for any costs or fees incurred as a result of alerts sent to email addresses or phone numbers connected with mobile or similar devices.

9.1.3 Alerts are not encrypted and will never include Customer's Access Devices or full Account number(s). However, alerts may include Customer's name and some information about Customer's Accounts, depending upon which alert(s) Customer selects. Anyone with access to Customer's email address will be able to view the contents of these alerts.

9.1.4

10. **Use of Financial Management (FM) Software.** Use of the Services may be supplemented by use of certain FM software. Compatibility and functionality of the FM software with the Services may vary depending upon the FM software Customer is using, and Bank makes no representations or guarantees regarding use of the Services with Customer's FM software. Customer is responsible for obtaining and maintaining the FM software. Customer's use of the FM software is governed by the software license agreement(s) included with each software application. Customer must agree to the terms and conditions of the software license agreement(s) during the installation of the FM software on Customer's Computer. Customer is responsible for the correct set-up and installation of the FM software, as well as maintenance, updates and upgrades to the FM software and/or Customer's Computer. Bank will provide Customer with reasonable assistance, when requested, to enable Customer's use of the Services with FM software. Bank is not responsible for any problems related to the FM software itself, Customer's Computer or Customer's ability to connect using the FM software as described in this Appendix. Customer should verify all Account data obtained and any transactions that may be executed on Customer's Accounts using FM software, as applicable. Bank's records of transactions, instructions and communications regarding Customer's Accounts and use of the Services supersede any records stored or created on Customer's Computer through the use of FM software. Customer is responsible for any and all obligations to any

software vendor arising from Customer's use of that vendor's FM software. Customer acknowledges and agrees that the FM software versions supported by Bank for purposes of use with the Services shall be in accordance with the sunset policy of the FM software provider.

11. Additional Security Terms. In addition to the other terms of this Appendix and of the parties' Cash Management Master Agreement, Customer agrees not to disclose any proprietary information regarding the Services to any third party (except to Customer's Administrator(s) and Authorized User(s)). Customer acknowledges that there can be no guarantee of secure transmissions over the Internet and agrees to comply with any operating and commercially reasonable security procedures Bank may establish from time to time with respect to the Services. Customer will be denied access to the Services if Customer fails to comply with any of these procedures. Customer is responsible for reviewing the transaction reports Bank provides on-line and in Customer's monthly statements to detect unauthorized or suspicious transactions. In addition to any other provision hereof regarding authorization of transactions using the Services or in the parties' Cash Management Master Agreement, all transactions will be deemed to be authorized by Customer and to be correctly executed thirty (30) Calendar Days after Bank first provides Customer with a statement or online transaction report showing that transaction, unless Customer has provided written notice that the transaction was unauthorized or erroneously executed within that period. In order to minimize risk of loss, Customer agrees to cause its Administrator or designated Authorized User(s) to review the transaction audit log available with the Services to detect unauthorized or erroneous transactions not less frequently than once every five (5) Calendar Days.

12. Terminating this Appendix; Liability.

12.1 This Appendix may be terminated in accordance with the terms and conditions of the Cash Management Master Agreement.

12.2 The provisions of this Appendix relating to Customer's and Bank's liability and the disclaimer of warranties set forth in the Cash Management Master Agreement and incorporated herein by reference shall survive the termination of this Appendix.

13. Changes to the Services and this Appendix. Bank may change the Services and this Appendix (including any amendments hereto) in accordance with the terms and conditions of the Cash Management Master Agreement.

14. Notices. Notices required by this Appendix shall be provided in accordance with the terms and conditions of the Cash Management Master Agreement.

15. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the Services and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK.



APPENDIX II

TD ACH ORIGINATION SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and the parties' Bank Internet System Agreement, as applicable. This Appendix applies to all automated clearing house ("ACH") Services made available to Customer, in Customer's capacity as an Originator, by Bank, as an Originating Depository Financial Institution ("ODFI"). All capitalized terms used herein without definition shall have the meanings given to them in either the Cash Management Master Agreement or the *NACHA Rules* (as defined below), as applicable. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. Services. The ACH network is a funds transfer system which provides for the interbank clearing of electronic credit and debit Entries for participating financial institutions. The ACH system is governed by the National Automated Clearing House Association's ("NACHA") *Operating Rules and Operating Guidelines* (collectively the "*NACHA Rules*").

2. Customer Obligations.

2.1 Customer will comply and shall cause its employees, officers, directors, agents and its Authorized Representative(s) and Administrator(s) to comply with (i) the *NACHA Rules* as amended from time to time and (ii) any specifications, advisories, interim policies, or instructions related to ACH transactions issued, from time to time, by Bank, NACHA or any federal or state regulatory authorities. The duties of Customer set forth in this Appendix in no way limit the requirement that Customer comply with the *NACHA Rules*. Customer specifically adopts and makes to Bank all representations and warranties of an Originator under the *NACHA Rules*, including that Customer will not initiate Entries in violation of the laws of the United States. Customer has access to a copy of the *NACHA Rules* and acknowledges receipt of a copy. (The *NACHA Rules* may be obtained at NACHA's website at www.NACHA.org or by contacting NACHA directly at 703-561-1100.) Customer agrees to subscribe to receive revisions to the *NACHA Rules* directly from NACHA.

2.2 Customer will maintain a checking Account ("Settlement Account") at Bank with available balances as of the Effective Entry Date sufficient to offset any Entries submitted and against which any rejected or returned Entries may be credited or debited. Bank reserves the right, in its sole and exclusive discretion and at any time, to require ACH pre-funding of credit Entries requested by Customer, in accordance with the terms and conditions of any agreement between Bank and Customer relating to pre-funding of such Entries, including as otherwise set forth in this Appendix. Bank also reserves the right, in its sole and exclusive discretion and at any time, to delayed settlement of debit Entries requested by

Customer, in accordance with the terms and conditions of any agreement between Bank and Customer relating thereto.

2.3 Customer agrees from time to time, upon Bank's request and in accordance with this Appendix and the parties' Cash Management Master Agreement, to promptly provide Bank with information pertaining to Customer's financial condition as Bank may request, including without limitation, the name(s) of other financial institutions that Customer is using to originate Entries.

2.4 Nothing in this Appendix or any course of dealing between Customer and Bank (i) constitutes a commitment or obligation of Bank to lend money to Customer, (ii) obligates Bank to extend any credit to Customer, to make a loan to Customer or otherwise to advance funds to Customer to pay for any payment order contrary to Bank's published availability schedules and the settlement timing as reflected herein, and in such other documents and materials as may be provided to Customer by Bank with regard to the Services from time to time, (iii) constitutes a modification of this Appendix, the *NACHA Rules*, or the Security Procedures, or (iv) otherwise constitutes an agreement between Bank and Customer regardless of whatever practices and procedures Bank and Customer may use.

2.5 Customer is responsible for all tariffs, duties or taxes (excluding U.S. federal, state and local taxation of the income of Bank) that may be imposed by any government or governmental agency in connection with any payment order executed pursuant to this Appendix, including without limitation any international tariffs, duties or taxes related to international ACH Entries as further described in Section 6 below.

2.6 Customer shall be liable for all fines including without limitation any international fines related to international ACH Entries as further described in Section 6 below, that may be incurred by Bank that are attributable to Customer's failure to comply with (i) the *NACHA Rules*, or (ii) the laws, regulations and orders administered by the U.S., including without limitation, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN").

3. Risk Exposure Limits.

3.1 Bank will establish for Customer, in Bank's sole and exclusive discretion, a transactional "Credit Exposure Limit" and a "Debit Exposure Limit" ("Exposure Limit(s)"). Each Exposure Limit will be established as an aggregate limit over multiple Settlement Dates with other not-yet-settled transactions issued by Customer through any ACH application with Bank. The Exposure Limits are based on Customer's financial condition and anticipated or historical level(s) of Entry instructions with Bank. Bank will notify Customer of Customer's Exposure Limits prior to implementation of the Services.

3.2 Customer shall promptly notify Bank if Customer anticipates a significant increase or decrease in the dollar amount of any of its ACH transactions. Bank may, from time to time, in its sole discretion, change the amount of Customer's Exposure Limits. Bank may, on an annual or more frequent basis, in Bank's sole discretion, review Customer's Exposure Limits and make any adjustments to Customer's Exposure Limits that Bank may deem appropriate. Bank will promptly notify Customer in writing of any adjustments to Customer's Exposure Limits.

3.3 Bank monitors all Exposure Limits for every customer that originates ACH transactions. Bank may suspend or reject processing of any Entry instructions if such Entry exceeds Customer's Exposure Limit(s). Bank may, in its sole and exclusive discretion, but shall have no obligation, to elect to process occasional Entry instructions that would exceed Customer's Exposure Limit(s). If Customer's Entry instructions exceed its Exposure Limit(s), Bank may elect to process such instructions subject to there being sufficient available funds in the Settlement Account, or in any other Customer Account(s) authorized by Bank for ACH transaction purposes, for the total amount of all credit Entries submitted to Bank for processing. In such event, Bank may elect to reduce available funds in the Settlement Account, as well as place a hold on available funds in any other Customer Account(s) authorized by Bank for ACH transaction purposes to the extent necessary to cover the total amount of the ACH credit Entries, on the Business Day that Bank begins processing Customer's ACH file. Customer's Settlement Account will be debited on the effective Settlement Date of the file, simultaneously with removal of the hold on funds in the other Customer Account(s). Alternatively, if Customer's Entry instructions exceed Customer's Exposure Limit(s), Bank may elect to process such instructions and release a file against insufficient collected funds, subject to Customer promptly depositing collected funds in the Settlement Account in the form of a cash deposit, wire transfer, intra-bank fund transfer or loan advance to cover Customer's funding obligation.

4. File Transmission Methods; Addenda.

4.1 Customer may elect, in accordance with the Services' Setup Form(s), to transmit a NACHA-formatted file to Bank via the following methods, or via such other

methods as Bank may permit from time to time in its sole and exclusive discretion:

4.1.1 **Bank Internet System Transmission.** Customer may transmit a NACHA-formatted file to Bank via the service described in the Bank Internet System Appendix. Customer agrees to the terms of the Bank Internet System Appendix and its related security procedures when initiating Entries as described therein.

4.1.2 **Direct Electronic Transmission.** Customer may transmit a NACHA-formatted file directly to Bank, as described in or as otherwise permitted by Bank's Appendix for Data Transmission Services. Connectivity between Bank and Customer must be established and successfully tested prior to live transactions.

4.2 **Electronic Data Interchange ("EDI").** EDI consists of the electronic movement of data between Customer and Bank in a structured, computer-retrievable data format that permits information to be transferred between a computer program at Customer's location and a computer program at Bank's location without re-keying. Customer and Bank may transmit between each other an ACH file that contains ACH Addenda which conform to the *NACHA Rules* via EDI, and as described in or as otherwise permitted by Bank's Appendix for Data Transmission Services. Bank will process and forward Addenda information along with financial transactions through the ACH network. Bank will, upon Customer's request, forward Addenda information to Customer within two (2) Business Days of Bank's receipt of such information.

5. Transmittal of Entries by Customer.

5.1 Customer will send file(s) of credit and debit Entries to Bank (i) with computer readable information; (ii) with an ACH file and format consistent with current NACHA file and Bank specifications; and (iii) on the medium as agreed by the parties and in accordance with the security procedures associated with that transmission medium. Customer agrees to initiate Entries described herein in accordance with the requirements of, and in compliance with its responsibilities, representations and warranties as an Originator under, the *NACHA Rules*. Bank shall comply with the *NACHA Rules*, and Bank specifically adopts and makes to Customer all representations and warranties of an ODFI under the *NACHA Rules*. Bank agrees to process Entries described herein in accordance with the requirements of, and in compliance with its responsibilities, representations and warranties as an ODFI under, the *NACHA Rules*.

5.2 With respect to any credit and debit Entries initiated and transmitted by Customer that involve consumers, each of Customer and Bank will comply with, each as may be amended from time to time: (i) all authorization, disclosure and other requirements of the *NACHA Rules* and (ii) all applicable federal and state laws and regulations, including, without limitation, any applicable requirements of Regulation E of the Consumer Financial Protection Bureau (or any successor entity who

administers Regulation E) (hereinafter "Regulation E") and the Federal Electronic Funds Transfer Act.

5.3 Customer acknowledges the right of a consumer Receiver of an unauthorized debit Entry, as applicable and as described in the *NACHA Rules*, to obtain a refund of the funds debited from Receiver's account by such Receiver sending a written notice to Receiver's Receiving Depository Financial Institution ("RDFI") in accordance with the *NACHA Rules* (i.e., a Written Statement of Unauthorized Debit), and where such notification is received in time and in a manner that reasonably allows the RDFI to meet the deadline for transmitting a Return Entry as provided in the *NACHA Rules*. Customer also acknowledges the right of a corporate Receiver of a debit Entry, as applicable and as described in the *NACHA Rules*, to obtain a refund of the funds debited from such Receiver's account by such Receiver sending a notice to Receiver's RDFI within two (2) Business Days following the Settlement Date of the original Entry. Customer indemnifies Bank against any such claim for a refund by any Receiver.

5.4 In accordance with this Appendix, Customer may use the Services to initiate and transmit credit and debit Entries with certain Standard Entry Class ("SEC") Codes. Authorized SEC Codes include PPD, PPD+, CCD, CCD+ and CTX. All other SEC Codes may be used with proper designation on the Services' Setup Form(s) and in accordance with additional instructions from and requirements by Bank, as applicable. Bank may also suspend or terminate Customer's use of one or more SEC Codes at any time in Bank's sole and exclusive discretion.

5.5 Bank may suspend Customer's use of one or more inactive ACH set-ups after 12 months of inactivity and subsequently terminate Customer's use of the inactive ACH set-up on one or more channels of delivery, after 16 months of inactivity. Non-use of ACH Origination for 16 months, may result in the termination and removal of the ACH Service.

6. International ACH Transactions ("IAT Entries").

6.1 An IAT Entry is a debit or credit Entry that is part of a payment transaction involving a Financial Agency located outside of the territorial borders of the United States, which is processed through the domestic ACH network, pursuant to the *NACHA Rules*, including the rules pertaining to International ACH Transactions. IAT Entries also include those that are funded directly by an incoming international wire or similar funding source. The *NACHA Rules* establish SEC Code "IAT" for all International ACH Transactions. Customer agrees to be bound by the *NACHA Rules* and all other statutes and regulations pertaining to IAT Entries, including all applicable OFAC and FinCEN rules and regulations associated with IAT Entries. Customer acknowledges that IAT Entries require additional mandatory information, according to special formatting requirements, in the computer record for such Entries within an ACH batch file. Customer expressly agrees to identify and properly initiate all IAT Entries. Bank will facilitate IAT Entries to Receivers located in foreign countries approved by Bank and

facilitated by the ACH or the Gateway Operator (hereinafter in this Section, collectively, "ACH Operator"). Bank will process each IAT Entry in accordance with (a) the laws and payment system rules and requirements of the receiving foreign country ("Foreign Country Rules"), (b) any agreement governing IAT Entries between Bank and the ACH Operator through which Bank processes the IAT Entry, the terms of which Bank communicates to Customer prior to Customer's use of the Services or from time thereafter, and (c) the *NACHA Rules*.

6.2 Customer acknowledges and agrees that IAT Entries may be subject to laws, regulations and restrictions of U.S. and foreign governments relating to foreign exchange transactions. Before initiating an IAT Entry, Customer agrees to understand and accept the Foreign Country Rules. An IAT Entry must be authorized by the Receiver. The form and content of the Receiver's authorization, including whether such authorization is oral, electronic or written, is governed by Foreign Country Rules. Customer assumes the risk of rejection of its Entries according to Foreign Country Rules, Bank and the ACH Operator. Customer expressly acknowledges and agrees that Outbound IAT Entries, once transmitted, are irrevocable and are subject to the Foreign Country Rules; furthermore, the time frames for return of an Entry are determined by the Foreign Country Rules and may exceed the sixty (60) day return window for consumer Entries defined by the U.S. ACH system and the *NACHA Rules*, as well as the return window for non-consumer Entries. Customer also agrees that IAT Entries may not be dishonored, reversed or settled upon a specific date, and that pre-notifications are not permitted with respect to IAT Entries involving certain foreign countries. To the extent not otherwise prohibited by law, in connection with IAT Entries, (1) Customer assumes the risk of all fluctuations in foreign exchange rates or availability, and (2) Customer assumes the risk of loss for creating any and all erroneous IAT Entries. Customer acknowledges and agrees that the processing, settlement and/or availability of such Entries may be delayed or suspended in the event that Bank determines that enhanced scrutiny or verification of such Entries is necessary under the *NACHA Rules* and/or applicable U.S. law. The ACH Operator through which Bank processes the IAT Entry, in its sole discretion, may also refuse to handle IAT Entries. Customer acknowledges that Bank shall have no liability for such delay or refusal.

6.3 In addition to the provisions of Section 22 of this Appendix, Customer makes the following additional representations and warranties with respect to any IAT Entry submitted by Customer or on Customer's behalf:

6.3.1 Customer is in compliance with U.S. law, including, but not limited to, Customer's obligations under programs administered by OFAC and FinCEN; and

6.3.2 The origination of an Outbound IAT Entry is in compliance with the Foreign Country Rules, including any requirements regarding authorization with respect to an IAT Entry.

6.4 Bank will not be liable for (a) any failure or delay by the ACH Operator, any intermediary financial institution, or the financial institution designated to receive the IAT Entry in the receiving country in processing or failing to process any IAT Entry that is transmitted to the receiving country, or (b) the acts or omissions by a third party, including without limitation, the delay or failure of any third party to process, credit or debit any IAT Entry. Bank is also not responsible for the transmission or settlement of IAT Entries on foreign holidays or other days on which foreign countries may not process Entries.

6.5 With respect to credit IAT Entries that Customer wishes to originate in the currency of a designated foreign government or intergovernmental organization ("Foreign Currency"), Bank will originate the IAT Entries in U.S. dollars ("USD") only. Once the Entry is transmitted by Bank to the ACH Operator, the ACH Operator will convert the amount to be transferred from USD to the Foreign Currency. If the financial institution designated to receive the funds does not pay the Receiver specified in the Entry, or if the Entry is subsequently determined to be erroneous, the ACH Operator will convert the amount to be returned from the Foreign Currency to USD. Bank will not be liable for any difference in the amount of the original Entry after it has been converted from the Foreign Currency to USD. Further, if Customer designates the currency to arrive at the receiving financial institution in Foreign Currency, and the designated Receiver account at the receiving financial institution is a USD account, Customer acknowledges that the receiving financial institution may: (1) elect to convert the currency back to USD and post the transfer to the Receiver's account accordingly, or (2) return the Entry, in which case the amount transferred is converted from Foreign Currency back to USD to post back to Customer's account. Customer assumes all foreign exchange risk associated with any of the foregoing.

7. Security Procedures.

7.1 Customer and Bank shall comply with the security procedures set forth or incorporated by reference in this Appendix, the Cash Management Master Agreement, the Bank Internet System Appendix, Data Transmission Services Appendix and/or associated documents provided by Bank, including without limitation the Services' Setup Form(s) (collectively the "Security Procedures"), with respect to Entries transmitted by Customer to Bank. Customer acknowledges and agrees the Security Procedures are a commercially reasonable method for the purpose of verifying the authenticity of Entries (or any request for cancellation or amendment thereof). Customer further acknowledges that the purpose of the Security Procedures is not to detect an error in the transmission or content of an Entry. No security procedures have been agreed upon between Bank and Customer for the detection of any such error.

7.2 Customer is strictly responsible for establishing, implementing, maintaining and (as appropriate) updating its own security procedures (a) to safeguard against unauthorized transmissions, and (b) relating to the initiation, processing and storage of Entries. As required by the *NACHA*

Rules with respect to the protection of ACH information (non-public information, including financial information of Receivers and Customer's customers, used to create, or contained within, an ACH Entry and any related addenda record), Customer shall ensure that its security policies, procedures and systems:

- Protect the confidentiality and integrity of the protected information,
- Protect against anticipated threats or hazards to the security or integrity of protected information until its destruction, and
- Protect against unauthorized use of protected information that could result in substantial harm to the Receiver/customer.
- Abide by all rules pertaining to commercially reasonable data security as prescribed within the *NACHA Rules*

Customer warrants to Bank that no individual will be allowed to initiate transfers in the absence of proper supervision and safeguards, and Customer agrees to take reasonable steps to maintain the confidentiality of the Security Procedures and any passwords, codes, security devices and related instructions Bank provides in connection with the Security Procedures. If Customer believes or suspects that any such information or instructions have been known or accessed by an unauthorized person, Customer agrees to notify Bank immediately by calling 1-866-475-7262, followed by written confirmation to TD Bank, N.A., Attn: Treasury Management Services Support, 6000 Atrium Way, Mt. Laurel, New Jersey, 08054. The occurrence of unauthorized access will not affect any transfers Bank makes in good faith prior to, and within a reasonable time period after, its receipt of such notification.

7.3 Bank may, from time to time, propose additional or enhanced security procedures to Customer. Customer understands and agrees that if it declines to use any such enhanced procedures, it will be liable for any losses that would have been prevented by such procedures. Notwithstanding anything else contained in this Appendix, if Bank believes immediate action is required for the security of Bank or Customer funds, Bank may initiate additional security procedures immediately and provide prompt subsequent notice thereof to Customer.

8. Compliance with Security Procedures.

8.1 If an Entry (or a request for cancellation or amendment of an Entry) received by Bank purports to have been transmitted or authorized by Customer, it will be deemed effective as Customer's Entry (or request), and Customer shall be obligated to pay Bank the amount of such Entry (or request) even though the Entry (or request) was not authorized by Customer, provided Bank acted in compliance with the Security Procedures.

8.2 If an Entry (or a request for cancellation or amendment of an Entry) received by Bank was transmitted or authorized by Customer, Customer shall be obligated to pay the amount of the Entry as provided herein, whether or not Bank complied with the Security Procedures and whether or not that Entry was erroneous in any respect

or that error would have been detected if Bank had complied with the Security Procedures.

9. Recording and Use of Communications. Customer and Bank agree that all telephone conversations or data transmissions between them or their agents made in connection with this Appendix may be electronically recorded and retained by either party by use of any reasonable means.

10. Processing, Transmittal and Settlement of Entries by Bank.

10.1 Bank will process, transmit and settle for credit and debit Entries initiated by Customer as provided in the *NACHA Rules* as in effect from time to time, and pursuant to this Appendix. Exclusive of "Same Day ACH Entries," which are described in Section 23 below, Bank will transmit such Entries as an ODFI to the ACH Operator by the deadline of the ACH Operator, provided such Entries are received by Bank prior to 8:00 p.m. Eastern Time ("ET") and the ACH Operator is open for business on such Business Day. Entries received after 8:00 p.m. ET will be deemed received the following Business Day. If the Effective Entry Date falls on a non-Business Day, final settlement will occur on the next Business Day. Customer may submit a NACHA-formatted file up to the time limit in advance of the Effective Entry Date as the Services permit, or as may otherwise be permitted by Bank under the terms of this Appendix. Customer will hold Bank harmless from all charges and liabilities that may be incurred as a result of the delivery of late Entries.

10.2 If the file of Entries is received other than in specified NACHA and Bank format, Customer will be required to provide Bank with a corrected file. If a corrected file of Entries is received later than 8:00 p.m. ET on the delivery date with an intended Effective Entry Date of next-Business Day, Customer will hold Bank harmless from all charges and liabilities that may be incurred as a result of the processing of late Entries.

10.3 For purposes of this Appendix, Entries shall be deemed received by Bank, in the case of electronic file transmission, when the transmission is completed as set forth in Bank's Appendix for Data Transmission Services and/or the Services' Setup Form(s).

10.4 If any of the requirements of this Section 10 (or of Section 23 with respect to Same Day ACH Entries) are not met, Bank shall use reasonable efforts to transmit such Entries to the ACH Operator by the next deposit deadline on which the ACH Operator is open for business. Any stale dated Effective Entry Date, may result in "Same Day ACH Entries".

11. On-Us Entries. Except as otherwise provided herein, in the case of an Entry received for credit or debit to an account maintained by Bank (an "On-Us Entry"), Bank will credit or debit the Receiver's account in the amount of such Entry on the Effective Entry Date, provided the requirements set forth herein are otherwise met. If those requirements are not met, by reason of stale or same-day Effective Entry Dates on such Entries, Bank will credit or

debit the Receiver's account in the amount of such Entry on the date the Entry was received by Bank, or if the Entry was received on a non-Business Day, Bank will credit or debit the Receiver's account in the amount of such Entry on the next Banking Day following the date the Entry was received by Bank. Bank will have the right to reject an On-Us Entry as described in Section 12, *Returned or Rejected Entries*. In the case of an On-Us Entry, Bank will have all rights of an RDFI including, without limitation, the rights set forth in *NACHA Rules*.

12. Returned or Rejected Entries.

12.1 In the event any Entry is returned or rejected by the ACH Operator or any RDFI or Intermediary Depository Financial Institution, it shall be the responsibility of Customer to (i) remake and resubmit such Entry, (ii) with respect to an ACH Debit Entry, enroll in Bank's Auto-Redeposit service or (iii) otherwise resolve the returned Entry in accordance with the *NACHA Rules*.

12.2 Bank shall remake such Entry in any case where rejection by the ACH Operator was due to mishandling of such Entry by Bank and sufficient data is available to Bank to permit it to remake such Entry. In all other instances, Bank's responsibility will be to receive rejected or returned Entries from the ACH Operator, perform necessary processing, control and settlement functions, and to forward such Entries to Customer. Except for an Entry retransmitted by Customer in accordance with the requirements of Section 5, *Transmittal of Entries by Customer*, or the enrollment in Bank's Auto-Redeposit service for ACH Debit Entries, Bank shall have no obligation to retransmit a returned Entry to the ACH Operator if Bank complied with the terms of this Appendix and the *NACHA Rules* with respect to the original Entry and the rejection was not due to mishandling of such Entry by Bank.

12.3 Bank may reject any Entry which does not comply with the requirements of Section 5, *Transmittal of Entries by Customer*, or Section 7, *Security Procedures*. Bank may also reject any Entry which contains a future Settlement Date that exceeds the limits set forth within the Services. Bank may reject an On-Us Entry for any reason for which an Entry may be returned under the *NACHA Rules*. Bank may reject any Entry or file if Customer has failed to comply with its Settlement Account balance obligations under Section 2, *Customer Obligations*, or Customer's Exposure Limit under Section 3, *Risk Exposure Limits*. Notices of rejection shall be effective when given. Bank shall have no liability to Customer by reasons of the rejection of any such Entry or the fact that such notice is not given at an earlier time than that provided for herein. Bank may monitor Customer's rejected or returned Entries. Bank reserves the right, in its sole and exclusive discretion, to require Customer to establish a reserve Account in the event that an excessive number of Customer's debit Entries are rejected or returned.

12.4 In accordance with *NACHA Rules*, Bank may monitor returned Entries, and in its sole discretion, may: (1) require Customer to lower its return rates, (2) invoke premium penalty fees for unauthorized or excessive return rates, and/or (3) invoke termination or suspension of the

Services and/or this Appendix in conjunction with Section 31 of this Appendix.

12.5 In Bank's sole discretion, and upon Customer request, Bank may enroll eligible customers in the ACH Auto-Redeposit service for ACH debit origination. The service automates Customers redeposit of eligible returns due to insufficient funds (R01) and uncollected funds (R09), one or two additional times, within nine (9) calendar days as selected by Customer at the time of enrollment in the service. Customer will receive notice of each return attempt and be responsible for any associated fees. Customer's account will be setoff for the amount of the returned Debit Entry after the final attempt to Auto-Redeposit the Entry is determined by Bank to be unsuccessful.

13. **Cancellation or Amendment by Customer.** Customer shall have no right to cancel or amend any Entry or file after its receipt by Bank. However, if such request complies with the Security Procedures applicable to the cancellation of data, Bank shall use reasonable efforts to act on a request by Customer for cancellation of an Entry prior to transmitting it to the ACH Operator, or in the case of an On-Us Entry, prior to crediting or debiting a Receiver's account, but Bank shall have no liability if such cancellation is not effected. Customer shall reimburse Bank for any expenses, losses, or damages Bank may incur in effecting or attempting to effect the cancellation or amendment of an Entry.

14. **Reversing Entries/Files.** If Customer discovers that any Entry or file Customer has initiated was in error, it may use the Services to correct the Entry or file by initiating a reversal or adjustment, or Customer may notify Bank of such error and Bank will utilize reasonable efforts on behalf of Customer, consistent with the *NACHA Rules*, to correct the Entry or file by initiating a reversal or adjustment of such Entry or file. In all such cases, it shall be the responsibility of Customer to notify the affected Receiver that an Entry or file has been made which is at variance with the authorization or is otherwise erroneous. Customer indemnifies Bank against any claim by any Receiver that a reversing Entry or file requested by Customer is wrongful. Customer understands and acknowledges that certain RDFIs may not or cannot comply with such reversal and that, in such an event, Bank will debit Customer's Settlement Account in the amount of the provisional credit applied to the Settlement Account for such Entry or file.

15. **Notice of Returned Entries.** Bank will use reasonable efforts to notify Customer by electronic transmission of the receipt of a returned Entry from the ACH Operator no later than one (1) Business Day after the Business Day of such receipt. Except for an Entry re-transmitted by Customer in accordance with the requirements of Section 5, *Transmittal of Entries by Customer*, or the enrollment in Bank's Auto-Redeposit service for ACH Debit Entries, Bank shall have no obligation to re-transmit a returned Entry to the ACH Operator if Bank complied with the terms of this Appendix with respect to the original Entry.

16. **Notifications of Change.** Bank will use reasonable efforts to notify Customer of each Notification of Change ("NOC") or Corrected Notification of Change ("Corrected NOC") received by Bank related to Entries transmitted by Customer within two (2) Business Days after receipt thereof. Customer shall ensure that changes requested by the NOC or Corrected NOC are made within six (6) Business Days of Customer's receipt of the NOC or Corrected NOC information from Bank or prior to initiating another Entry to the Receiver's account, whichever is later.

In the event that Customer has not updated the NOC, the Bank will undertake this correction on the Customer's behalf, before each subsequent Entry is placed into the Network, in order to be compliant with the *NACHA Rules*. Bank will access a fee for updating the NOC as outlined in the fee schedule.

17. **Pre-Notification and Rejection of Pre-Notification.** Bank recommends that, as permitted by the *NACHA Rules* or applicable law, Customer send pre-notifications at least three (3) Business Days prior to initiating an authorized Entry to a particular account in a format and medium approved by the *NACHA Rules*. Customer may also initiate a new pre-notification (i) when any changes are made to an account number, financial institution, or individual identification number or (ii) as otherwise stated in the *NACHA Rules*. Customer understands and acknowledges that once a pre-notification has been initiated using the Services, Customer will be restricted from initiating any Entry to such customer(s) for three (3) Business Days.

18. **Participant Authorization for Entries.**

18.1 To the extent required by the *NACHA Rules* or applicable law, Customer will obtain all consents and written authorizations for all Entries in accordance therewith. Such authorizations and any related disclosures shall be in a form that complies with (i) all requirements of the *NACHA Rules* and (ii) all applicable federal and state laws and regulations, as the same may be amended from time to time, including, without limitation, any applicable requirements of Regulation E, the Federal Electronic Funds Transfer Act, and sanctions enforced by OFAC. Customer shall obtain and maintain current information regarding OFAC enforced sanctions. (This information may be obtained directly from the OFAC Compliance Hotline at (800) 540-OFAC or by visiting the OFAC website at www.ustreas.gov/ofac.) Each Entry will be made according to such authorization and shall comply with the *NACHA Rules*. No Entry will be initiated by Customer after such authorization has been revoked or the arrangement between Customer and such Receiver or other party has terminated.

18.2 Customer shall retain all consents and authorizations for the period required by the *NACHA Rules*. Customer will furnish to Receiver, or to Bank upon its request, an original or a copy of an authorization as required under or for any purpose required by the *NACHA Rules*. No investigation or verification procedure undertaken by Bank shall be deemed to limit or waive Customer's obligations under this Section.

19. Re-initiation of Entries. Customer may not re-initiate Entries except as prescribed by the *NACHA Rules*.

20. Payment by Customer for Entries; Payment by Bank for Entries.

20.1 Except as may otherwise be agreed by Bank in its sole and exclusive discretion, Customer shall pay Bank the amount of each credit Entry transmitted by Bank pursuant to this Appendix at such time on the date of transmittal by Bank of such credit Entry as Bank, in its discretion, may determine.

20.2 Customer shall promptly pay Bank the amount of each debit Entry returned by an RDFI pursuant to this Appendix.

20.3 Bank will pay Customer the amount of each debit Entry transmitted by Bank pursuant to this Appendix at such time on the Settlement Date with respect to such debit Entry as Bank, in its discretion, may determine, and the amount of each On-Us Entry at such time on the Effective Entry Date as Bank, in its discretion, may determine.

20.4 Bank will use reasonable efforts to promptly pay Customer the amount of each credit Entry returned by an RDFI that was transmitted by Bank pursuant to this Appendix.

20.5 Customer acknowledges and agrees that any failure of Customer to make payment to Bank as described in this Section may constitute an event of default under any other agreement for credit that Customer or any of Customer's Affiliates has with Bank or any Affiliate of Bank. Customer further acknowledges and agrees to execute and deliver any further documents and instruments as Bank may require to effectuate the cross-default contemplated hereby.

21. Third-Party Service Provider; Third-Party Sender Activities.

21.1 Subject to Bank's prior approval and in its sole and exclusive discretion, Customer may appoint a third party to act as Customer's agent to process Entries on Customer's behalf and for purposes of the services provided hereunder ("Third-Party Service Provider"), as set forth in the Services' Setup Form(s). All data received by Bank from Third-Party Service Provider, including Entries and instructions (and corrections or adjustments thereto), are hereby authorized by Customer. All acts and omissions of Third-Party Service Provider shall be the acts, omissions and responsibility of Customer and shall be governed by the provisions of this Appendix. Customer agrees, jointly and severally with Third-Party Service Provider, to indemnify and hold Bank harmless from any and all liabilities, losses, damages, costs and expenses of any kind (including, without limitation, the reasonable fees and disbursements of counsel in connection with any investigative, administrative or judicial proceedings, whether or not Bank shall be designated a party thereto) which may be incurred by Bank

relating to or arising out of the acts or omissions of Third-Party Service Provider on behalf of Customer. Customer and Third-Party Service Provider shall execute any such other agreement(s) or documents as deemed necessary or appropriate by Bank prior to the initiation or continuation by Third-Party Service Provider of any services on Customer's behalf, including without limitation Bank's Third-Party Service Provider Agreement, as the same may be modified by Bank from time to time. Notice of any termination of Third-Party Service Provider's authority to transmit data and instructions to Bank on Customer's behalf shall be given to Bank in writing. The effective date of such termination shall be ten (10) Business Days after Bank receives written notice of such termination. Customer agrees that Bank retains the right to reject any Third-Party Service Provider and any Entries initiated by Customer's Third-Party Service Provider in its sole discretion.

21.2 Customer may not use the services provided hereunder to process Entries on behalf of Customer's clients (defined as a "Third-Party Sender" under the *NACHA Rules*), except where Customer has formally requested to engage in such activity in advance and where Bank has provided its prior approval, which Bank may grant or withhold in its sole and exclusive discretion. In the event Bank approves of such use, Customer shall execute such other agreement(s) or documents as deemed necessary or appropriate by Bank prior to the initiation or continuation by Customer of any ACH services in the capacity of a Third-Party Sender. Customer agrees that Bank retains the right to reject any request by Customer to engage in Third-Party Sender activities as well as any Entries initiated by Customer in such capacity, in Bank's sole discretion.

22. Customer Representations and Agreements; Indemnity. In addition to Customer representations, agreements and warranties otherwise described in this Appendix, Customer further represents and warrants to Bank and agrees, with respect to each and every Entry transmitted by Customer or any Third-Party Service Provider on Customer's behalf, that:

(i) Each person shown as the Receiver of an Entry received by Bank from Customer has authorized the initiation of such Entry and the crediting or debiting of its account in the amount and on the Effective Entry Date shown on such Entry;

(ii) Such authorization is operative at the time of transmittal or crediting or debiting by Bank as provided herein;

(iii) Entries transmitted to Bank by Customer are limited as set forth in Sections 3 and 5;

(iv) Customer shall perform its obligations under this Appendix in accordance with the laws of the United States and all other applicable laws, regulations and orders, including, but not limited to, the transaction screening and sanctions laws, regulations and orders administered by OFAC; laws, regulations and orders administered by FinCEN; and any state laws, regulations or orders applicable to the Originators of ACH transactions;

(v) Customer shall be bound by and comply with the provisions of the *NACHA Rules* (among other provisions of the *NACHA Rules*) that make payments of an Entry by the RDFI to the Receiver provisional until receipt by the RDFI of final settlement for such Entry;

(vi) Customer specifically acknowledges that it has received notice of the rule regarding provisional payment and of the fact that, if such settlement is not received, the RDFI shall be entitled to a refund from the Receiver of the amount of the Entry;

(vii) with respect to each International ACH Transaction ("IAT") that Customer may be permitted by Bank to initiate, Customer shall (a) classify and format payments transmitted to or received from a financial agency outside the U.S. as an IAT in accordance with the *NACHA Rules*, (b) provide data necessary to accompany the transaction in compliance with the Bank Secrecy Act's "Travel Rule," (c) screen the IAT prior to transmitting any file(s) of Entries to the Bank in accordance with the requirements of OFAC and comply with OFAC sanctions, and (d) otherwise comply with and be subject to all other requirements of U.S. law, the *NACHA Rules*, OFAC and FinCEN, as well as the Foreign Country Rules;

(viii) with respect to each Internet-initiated/mobile ("WEB") (as defined under the *NACHA Rules*) ACH Entry that Customer may be permitted by Bank to initiate, (a) Customer employs (1) commercially reasonable detection systems to minimize risk of fraud related to Internet-initiated payments, (2) commercially reasonable procedures to verify validity of routing numbers, (3) commercially reasonable methods of authentication to verify the identity of the Receiver, and (4) a commercially reasonable level of encryption technology, and (b) where required by the *NACHA Rules* and/or Bank, Customer conducts annual audits as to its security practices and procedures that include, at a minimum, verification of adequate levels of (1) physical security to protect against theft, tampering, or damage, (2) personnel and access controls to protect against unauthorized access and use and (3) network security to ensure secure capture, storage, and distribution, and will provide proof of such audits to Bank upon request;

(ix) with respect to each Telephone-Initiated ("TEL") Entry that Customer may be permitted by Bank to initiate, Customer has (a) employed commercially reasonable procedures to verify the identity of the Receiver, and (b) utilized commercially reasonable procedures to verify that routing numbers are valid;

(x) with respect to each Accounts Receivable ("ARC") Entry that Customer may be permitted by Bank to initiate, (a) the amount of the Entry, the routing number, the account number and the check serial number are in accordance with the source document, (b) Customer will retain a reproducible, legible image, microfilm or copy of the front of the Receiver's source document for each ARC Entry for two (2) years from the Settlement Date of the ARC Entry, (c) Customer has employed commercially reasonable procedures to securely store (1) all source documents until

destruction and (2) all banking information relating to ARC Entries, (d) Customer has established reasonable procedures under which the Receiver may notify Customer that receipt of Receiver's checks does not constitute authorization for ARC Entries to the Receiver's account and that Customer will allow the Receiver to opt-out of check conversion activity, and (e) the source document to which each ARC Entry relates may not be presented or returned such that any person will be required to make payment based on the source document unless the ARC Entry is returned;

(xi) with respect to each Back Office Conversion ("BOC") Entry that Customer may be permitted by Bank to initiate, (a) Customer has employed commercially reasonable procedures to verify the identity of the Receiver, (b) Customer has established and maintains a working telephone number for Receiver inquiries regarding the transaction that is answered during normal business hours and that such number is displayed on the notice required by the *NACHA Rules* for BOC Entries, (c) the amount of the Entry, the routing number, the account number and the check serial number are in accordance with the source document, (d) Customer will retain a reproducible, legible image, microfilm or copy of the front of the Receiver's source document for each BOC Entry for two (2) years from the Settlement Date of the BOC Entry, (e) Customer has employed commercially reasonable procedures to securely store (1) all source documents until destruction and (2) all banking information relating to BOC Entries, and (f) the source document to which each BOC Entry relates will not be presented or returned such that any person will be required to make payment based on the source document unless the BOC Entry is returned;

(xii) with respect to each Point-of-Purchase ("POP") Entry that Customer may be permitted by Bank to initiate, the source document provided to Customer for use in obtaining the Receiver's routing number, account number, and check serial number for the initiation of the POP Entry (a) is returned voided to the Receiver after use by Customer and (b) has not been provided to the Receiver for use in any prior POP Entry; and

(xiii) with respect to each Returned Check ("RCK") Entry that Customer may be permitted by Bank to initiate, (a) all signatures on the item are authentic and authorized, (b) the item has not been altered, (c) the item is not subject to a defense or claim, (d) the Entry accurately reflects the item, (e) the item will not be presented unless the related Entry has been returned by the RDFI, (f) the information encoded after issue in magnetic ink on the item is correct, and (g) any restrictive endorsement placed on the item is void or ineffective.

Customer shall indemnify and hold Bank harmless from any loss, liability or expense (including reasonable attorneys' fees and costs) resulting from or arising out of any breach of the foregoing warranties, representations or agreements. Customer shall also indemnify and hold Bank harmless from any claim of any person that Bank is responsible for any acts or omissions of Customer regarding any Entry received from Customer, or those of any other person related thereto, including, without limitation, any Federal Reserve Bank, ACH

Operator or transmission or communications facility, any Receiver or RDFI.

23. Same Day ACH ("SDA"). Customer may be permitted, in Bank's sole and exclusive discretion, to initiate SDA Entries. In the event Bank approves Customer's initiation of SDA Entries, either on a one time or other periodic basis, Customer agrees as follows:

23.1 Customer shall be solely responsible for transmitting its SDA Entries with the appropriate intended Effective Entry Date to qualify as an SDA Entry under the *NACHA Rules*.

23.2 Customer shall only initiate individual Entries that comply with the transaction limit per SDA Entry, as provided in the *NACHA Rules*

23.3 Customer will not initiate an SDA Entry as an IAT, as IATs are not eligible for same-day processing under the *NACHA Rules*.

23.4 Customer will transmit its SDA Entries to Bank in accordance with Bank's SDA Entry processing deadlines, as established by Bank from time to time and disclosed to Customer.

23.5 Customer acknowledges and agrees that if Customer sends an Entry with a stale or invalid Effective Entry Date, such Entry may be deemed and processed by Bank as an SDA Entry if transmitted in accordance with Bank's SDA Entry processing deadlines.

23.6 Customer acknowledges and agrees that if any of the requirements of this Section 23 are not met, including without limitation a failure by Customer to meet Bank's or the ACH Operator's deadline for SDA, Bank shall use reasonable efforts to transmit such Entries to the ACH Operator by the next available processing deadline on which the ACH Operator is open for business.

23.7 Customer further acknowledges that Bank will not consider the content of the Company Descriptive Date indicator when determining Customer's intent for processing and settlement of SDA Entries.

23.8 Customer will not initiate SDA Entries that are otherwise ineligible for SDA Entry processing and settlement in accordance with the *NACHA Rules*.

23.9 Customer otherwise agrees to and will comply with all other requirements under the *NACHA Rules* and by Bank with respect to SDA Entries, including as the same may be amended from time to time.

23.10 Customer will indemnify and hold Bank harmless from any SDA Entry processing and settlement that is performed by Bank as described herein and in accordance with the *NACHA Rules*, notwithstanding Customer's intent.

23.11 Customer will indemnify and hold Bank harmless from any intended SDA Entry not meeting the ACH Operator deadline due to Customer delays, or due to

Bank processing delays that are beyond Bank's reasonable control.

24. Inconsistency of Name and Account Number. Customer acknowledges and agrees that if an Entry describes a Receiver inconsistently by name and account number, then (i) payment of such Entry transmitted to an RDFI may be made by the RDFI (or by Bank for an On-Us Entry) on the basis of the account number, even if it identifies a person different from the named Receiver and (ii) Customer's obligation to pay the amount of Entry to Bank is not excused in such circumstances. Similarly, if an Entry describes an RDFI inconsistently by name and routing number, payment of such Entry may be made based on the routing number, and Customer shall be liable to pay that Entry.

25. Banks Unable to Accept ACH Transactions. If Customer submits an Entry to Bank relating to an RDFI which is not a participant in the ACH, then (i) Bank may reject such Entry and use reasonable efforts to notify Customer of such rejection or (ii) if Bank does not reject such Entry, upon receiving a return transaction related to the Entry from the ACH Operator, Bank may offset the Settlement Account and notify Customer of such transaction.

26. Notices, Instructions, Etc.

26.1 Except as otherwise expressly provided herein, Bank shall not be required to act upon any notice or instruction received from Customer or any other person, or to provide any notice or advice to Customer or any other person with respect to any matter.

26.2 Bank shall be entitled to rely on any written notice or other written communication believed by it in good faith to be genuine and to have been provided in accordance with the provisions of the parties' Cash Management Master Agreement.

27. Data Retention. Customer shall retain data on file adequate to permit remaking of Entries for five (5) Business Days following the date of their transmittal by Bank as provided herein and shall provide such data to Bank upon request. Without limiting the generality of the foregoing provision, Customer specifically agrees to be bound by and comply with all applicable provisions of the *NACHA Rules* regarding the retention of documents or any record, including, without limitation, Customer's responsibilities to retain all items, source documents and records of authorization, in accordance with the *NACHA Rules*.

28. Data Breaches.

28.1 Each of Bank and Customer agrees that it will adopt and implement commercially reasonable policies, procedures and systems to provide security as to the information being transmitted and to receive, store, transmit and destroy data or information in a secure manner to prevent loss, theft, or unauthorized access to data or

information ("Data Breaches"), including but not limited to, Consumer-Level ACH Data.

28.2 Each of Bank and Customer agrees that it will promptly investigate any suspected Data Breaches and monitor its systems regularly for unauthorized intrusions.

28.3 Customer will provide timely and accurate notification to Bank by calling 1-866-475-7262 with regard to any Data Breaches when known or reasonably suspected by Customer, including but not limited to, Data Breaches to Consumer-Level ACH Data, and will take all reasonable measures, including, without limitation, retaining computer forensic experts, to determine the scope of any data or transactions affected by any Data Breaches, providing all such determinations to Bank.

29. **Audit.** Bank has the right to periodically audit Customer's compliance with the *NACHA Rules*, U.S. law and Bank policies, including, but not limited to, this Appendix.

30. **Records.** All electronic or other files, Entries, Security Procedures and related records used by Bank for transactions contemplated by this Appendix shall be and remain Bank's property. Bank may, in its sole discretion, make available such information upon Customer's request. Any expenses incurred by Bank in making such information available to Customer shall be paid by Customer.

31. **Termination.** The parties may terminate this Appendix in accordance with the terms and conditions of the parties' Cash Management Master Agreement. In addition, if Customer breaches the *NACHA Rules* or causes Bank to breach the *NACHA Rules*, this Appendix may be terminated or suspended by Bank upon ten (10) Business Days' notice, or such shorter period as may be provided in the parties' Cash Management Master Agreement. Any termination of this Appendix shall not affect any of Bank's rights and Customer's obligations with respect to Entries initiated by Customer prior to termination, the payment obligations of

Customer with respect to services performed by Bank prior to termination, or any other obligations or provisions that by the nature of their terms survive termination of this Appendix, including without limitation Sections 2, 5, 10, 12, 13, 14, 18, 20, 21, 22, 27, 32, 33 and 34.

32. **Cooperation in Loss Recovery Efforts.** In the event of any damages for which Customer or Bank may be liable to the other or to a third party relative to the Services, both parties shall undertake reasonable efforts to cooperate with the other, as permitted by applicable law, in performing loss recovery efforts and in connection with any actions that Customer or Bank may be obligated to defend or elects to pursue against a third party.

33. **Governing Law.** In addition to the terms and conditions of the parties' Cash Management Master Agreement, the parties agree that if any payment order governed by this Appendix is part of a funds transfer subject to the federal Electronic Funds Transfer Act, then all actions and disputes as between Customer, or any Third-Party Service Provider acting on Customer's behalf, and Bank shall be governed by Article 4-A of the New York Uniform Commercial Code, as varied by this Appendix.

34. **Effectiveness.** Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the services described herein and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.



APPENDIX III

TD WIRE TRANSFER SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement, and the parties' Bank Internet System Appendix, and applies to all TD Wire Transfer Services ("Services") made available to Customer by Bank via the Bank Internet System. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement or the Bank Internet System Appendix, as applicable. To the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, or with the terms and conditions of the Bank Internet System Appendix, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. Description of the Services.

1.1 The Services described in this Appendix provide Customer with the capability to transfer funds from specific Account(s) with Bank to other accounts (the "Recipient Account(s)") as directed via the Bank Internet System. The Recipient Account(s) may be Customer accounts or third-party accounts, and may be with Bank or with domestic or foreign third-party financial institutions. Customer may use the Services to initiate one-time wire transfers, or to create templates for wire transfers made on a repetitive basis which involve the same Customer Account and Recipient Account ("Repetitive Transfer(s)"). All wire transfers must be initiated by an Authorized Representative of Customer.

1.2 Prior to Customer's use of the Services, Customer must first agree to and transmit all instructions in accordance with all of the terms, conditions and security procedures associated with the Bank Internet System, as further set forth in the Cash Management Master Agreement, including the Bank Internet System Appendix.

2. Execution of Wire Transfers.

2.1 By submitting a wire transfer, Customer authorizes Bank to withdraw the amount of any requested wire transfer which Customer may authorize and instruct via the Bank Internet System, plus any applicable fees and charges, which may be withdrawn from Customer's designated Account or from the wire transfer amount. Subject to the terms of this Appendix, Bank will accept and execute a wire transfer received from Customer that has been authenticated by Bank and that is in conformity with the Security Procedure (as further described below), cut-off times and other requirements as described in this Appendix and associated Bank Setup Form(s) and other documentation.

2.2 All wire transfers to accounts at other depository institutions are transmitted using the Fedwire funds transfer system owned and operated by the Federal Reserve Bank, or a similar wire transfer system used primarily for funds transfers between financial institutions. Notwithstanding the foregoing or anything to the contrary in this Appendix, Bank may use any means of transmission,

funds transfer system, clearing house, intermediary or correspondent bank that Bank reasonably selects to transfer funds from time to time.

2.3 Each wire transfer must include the following information in addition to any information which Bank may require for proper identification and security purposes: (i) Account number from which the funds are to be withdrawn, (ii) amount to be transferred, (iii) currency type, (iv) Customer's address, (v) name and ABA routing number or SWIFT BIC of the payee's (i.e., beneficiary's) bank, and (vi) name, address and account number of the payee (i.e., beneficiary). In the event a wire transfer describes an account number for the payee that is in a name other than the designated payee, Bank may execute the wire transfer to the account number so designated notwithstanding such inconsistency.

2.4 Templates created by Customer for Repetitive Transfers are the sole and exclusive responsibility of Customer. Except as otherwise expressly prohibited or limited by law, Customer agrees to release and hold Bank harmless from any loss or liability which Customer may incur after Bank has executed a Repetitive Transfer, including without limitation, any loss due to Customer error in creating the Repetitive Transfer template.

3. Time of Execution.

3.1 Bank will execute each authenticated wire transfer that is in conformity with all security procedures, cut-off times and other requirements set forth herein. Bank may require additional authentication of any wire transfer request. Bank reserves the right to reject a wire transfer request that cannot be properly authenticated. Cut-off times may be established and changed by Bank from time to time. Instructions for wire transfers received after such cut-off times may be treated by Bank for all purposes as having been received on the following Business Day.

3.2 Except for future-dated wire transfers, domestic wire transfers (U.S.-based receivers) initiated and approved by Bank's cut-off time on a Business Day will be processed that same day if that day is also a Business Day for Bank's correspondent facility and the recipient bank; wire transfers initiated and approved after Bank's cut-off time for domestic wire transfers will be processed the next Business Day if that day is also a Business Day for Bank's correspondent facility and the recipient bank. Future-dated

domestic wire transfers will be initiated on the effective date requested by Customer, not on the date Customer entered the transaction using the Services.

3.3 Bank may handle wire transfers received from Customer in any order convenient to Bank, regardless of the order in which they are received.

4. International Wires.

4.1 International wire transfers (non-U.S. receivers) of foreign currency initiated and approved by Bank's cut-off time for international wire transfers of foreign currency on a Business Day, and an international wire transfer of U.S. currency initiated and approved by Bank's cut-off time for international wire transfers of U.S. currency on a Business Day, will be processed within the industry standard delivery time (in most, but not all cases, two (2) Business Days). Foreign wire transfers may be subject to delays based on time-zone issues; the remote location of the recipient bank; cultural differences with respect to holidays and times of observation, etc.; and incorrect or incomplete information supplied by Customer.

4.2 Bank shall send Customer's authorized and authenticated wire transfers to foreign banks through any bank which is a member of Bank's correspondent network. Neither Bank nor any of Bank's correspondents shall be liable for any errors, delays or defaults in the transfer of any messages in connection with such a foreign wire transfer by any means of transmission. Customer acknowledges that foreign currency wire transfers must be based on a currency that Bank trades and that all rates of exchange will be the rate in effect at the time of execution of the wire transfer order, or at any other rate as may be agreed to by the parties. If the financial institution designated to receive the funds does not pay the payee (beneficiary) specified in a wire transfer order that is payable in foreign currency and the funds are returned to Bank, Bank will not be liable for a sum in excess of the value of the funds after they have been converted from foreign currency to U.S. dollars at Bank's buy rate for exchange at the time the cancellation of the wire transfer order is confirmed by Bank, less any charges and expenses incurred by Bank. If Customer elects to initiate an international wire transfer in U.S. currency, Customer acknowledges that the receiving bank may elect to pay the payee (beneficiary) in foreign currency at an exchange rate determined by the receiving bank. Customer agrees to bear all risk of loss due to fluctuation in exchange rates, and Customer shall pay Bank any costs and expenses of foreign currency conversion at Bank's then-prevailing rates, terms and conditions. Customer is advised that Bank's prevailing exchange rates may be less favorable to Customer than market exchange rates.

4.3 Bank makes no guarantee or representation as to the availability of funds at the foreign destination. Bank makes no express or implied warranty as to the time or date the wire transfer will arrive at the receiving bank, the amount of any fees to be charged by the receiving bank, or the time or date the payee (beneficiary) will receive credit for funds.

4.4 Customer understands and acknowledges that if the named payee (beneficiary) does not

match the account at the receiving bank, there is a risk the payee may not receive the wired funds. If the transfer is not received or credited in a timely manner, Bank will follow normal and customary procedures to complete the wire transfer, determine the location of the wired funds and/or return the funds to Customer. If Bank is unable to determine that the funds have been credited to the payee's account or have the funds returned, Customer assumes all financial liability or risk of loss for the amount of the wire transfer.

4.5 International wire transfers are subject to any and all applicable regulations and restrictions of U.S. and foreign governments relating to foreign exchange transactions. Bank has no obligation to accept any international wire transfer(s) directed to or through persons, entities or countries restricted by government regulation or prior Bank experience with particular countries. To the extent not otherwise prohibited by law, in connection with any international wire transfer(s) involving a transfer to or from any country outside of the U.S., and except as otherwise expressly prohibited or limited by law, Customer agrees to release and hold Bank harmless from any loss or liability which Customer may incur after Bank has executed the international wire transfer(s), including without limitation, any loss due to failure of a foreign bank or intermediary to deliver the funds to a payee (beneficiary).

5. Cancellation and Amendment of a Wire.

5.1 An Authorized Representative may request that Bank attempt to cancel or amend a wire transfer previously received from Customer. If a cancellation or amendment request is received by Bank before the wire transfer is executed and with sufficient time to afford Bank an opportunity to act upon Customer's request, Bank may, on its own initiative but without obligation, make a good faith effort to act upon such request. In the event Customer's cancellation or amendment request is received after execution of Customer's wire transfer request, Bank will attempt to have the wire transfer returned. Notwithstanding the foregoing, Bank shall have no liability for the failure to effect a cancellation or amendment, and Bank makes no representation or warranty regarding Bank's ability to amend or cancel a wire transfer. Except as otherwise expressly prohibited or limited by law, Customer agrees to indemnify Bank against any loss, liability or expense which Bank incurs as a result of the request to cancel or amend a wire transfer and the actions Bank takes pursuant to such request. Without limiting the foregoing, Customer agrees to be responsible for any losses arising from currency conversions effected by Bank pursuant to any foreign currency wire transfer order previously received from Customer that Customer subsequently requests be cancelled or amended.

5.2 Customer acknowledges and agrees that after a wire transfer order authorized by Customer as described in this Appendix has been accepted by the payee's (beneficiary's) financial institution, return of such funds must be authorized by the beneficiary, and Bank has no responsibility to procure the return of such funds. If Customer asks Bank to recover funds which Bank has already transferred, Bank shall attempt to recover the funds as provided below, but Bank shall be under no obligation to recover such funds. If Customer deposits with Bank an amount reasonably determined in good faith by

Bank to approximate the costs and expenses (including reasonable attorney's fees) which Bank may incur in attempting to recover the funds transferred, Bank may, in its sole discretion make an attempt to recover the funds. In lieu of such a deposit, Bank may request Customer to provide a bond or other assurance of payment reasonably satisfactory to Bank. Upon such deposit, or the supplying of such other assurance, Bank may take such action as it deems reasonable under the circumstances, including, for example, sending a request to reverse the transfer to any financial institution that received such funds. In no event, however, shall Bank be deemed to have guaranteed or otherwise assured the recovery of any portion of the amount transferred, nor to have accepted responsibility for any amount transferred.

6. Notice of Rejection or Return. Bank shall have no liability for wire transfers sent by Bank as directed by Customer which cannot be completed or which are returned due to incorrect information furnished by Customer. Customer is required to fully complete payee (beneficiary) name, and address, as the payee (beneficiary) bank may elect to return an otherwise valid wire transfer for incomplete payee (beneficiary) information. Bank may reject or impose conditions that must be satisfied before it will accept Customer's instructions for any wire transfer, in its sole discretion, including without limitation Customer's violation of this Appendix, Customer's failure to maintain a sufficient Account balance, or Bank's belief that the wire transfer may not have in fact been authorized. A wire transfer may also be rejected by an intermediary or payee (beneficiary) bank other than Bank, or by operation of law. If a wire transfer is rejected by Bank, Bank will notify Customer by telephone, by electronic means, by facsimile or by mail, depending on the method of origination. Upon rejection or return, Bank shall have no further obligation to act upon a wire transfer, nor shall Bank have any liability to Customer due to rejection by another person in the wire transfer process, or the fact that notice was not given or was not given at an earlier time, or within any specified time of receipt, acceptance, execution or payment of any wire transfer.

7. Security Procedure.

7.1 Customer agrees that the security procedures used by Customer and set forth or incorporated by reference in this Appendix and/or associated documents, including but not limited to the Bank Internet System Appendix, are a commercially reasonable method of providing security against unauthorized wire transfers and for all other instructions from Customer to Bank (hereinafter the "Security Procedure"). Any wire transfer by Customer shall bind Customer, whether or not authorized, if transmitted in Customer's name and accepted by Bank in compliance with the Security Procedure. Customer also agrees that any election Customer may make to change or refuse the Security Procedure is at Customer's risk and that any loss resulting in whole or in part from such change or refusal will be Customer's responsibility.

7.2 Bank may, from time to time, modify the Security Procedure. Except as expressly provided otherwise in this Appendix or in the parties' Cash Management Master Agreement, any such changes generally will be effective immediately upon notice to Customer as described in the parties' Cash Management Master Agreement. Customer

will be deemed to accept any such changes if Customer accesses or uses any of the Services after the date on which the change becomes effective.

7.3 Bank may, from time to time, propose additional or enhanced security procedures to Customer. Customer understands and agrees that if it declines to use any such additional or enhanced procedures, it will be liable for any losses that would have been prevented by such procedures. Notwithstanding anything else contained in this Appendix, if Bank believes immediate action is required for security of Bank or Customer funds, Bank may initiate additional security procedures immediately and provide prompt subsequent notice thereof to Customer.

7.4 Customer hereby acknowledges that the Security Procedure is neither designed nor intended to detect errors in the content or verify the contents of a wire transfer by Customer. Accordingly, any errors contained in wire transfers from Customer shall be Customer's responsibility, and Customer shall be obligated to pay or repay (as the case may be) the amount of any such wire transfer. No security procedure for the detection of any such Customer error has been agreed upon between Bank and Customer.

7.5 Customer is strictly responsible for establishing and maintaining its own procedures to safeguard against unauthorized wire transfers. Customer covenants that no employee or other individual will be allowed to initiate wire transfers in the absence of proper authority, supervision and safeguards, and agrees to take reasonable steps to maintain the confidentiality of the Security Procedure and any Access Devices and related instructions provided by Bank in connection with any Security Procedure utilized by Bank and/or Customer. If Customer believes or suspects that any such Access Devices, Security Procedure, information or instructions have been disclosed to or accessed by unauthorized persons, Customer agrees to notify Bank immediately by calling 1-866-475-7262, followed by written confirmation to TD Bank, N.A., Attn: Treasury Management Services Support, 6000 Atrium Way, Mt. Laurel, New Jersey, 08054. The occurrence of unauthorized access will not affect any transfers made in good faith by Bank prior to receipt of such notification and within a reasonable time period thereafter.

8. Accuracy; Inconsistency of Receiving Beneficiary Name and Account Number. In submitting any order or related instructions, Customer shall be responsible for providing all necessary information required by Bank in conjunction with the Services. The Services are only designed to respond to information provided by Customer. Accordingly, any inaccuracy in any information provided by Customer may result in an unintended transfer of funds. Bank bears no responsibility and shall not be liable to Customer for any information provided by Customer in an order or related instructions that are inaccurate, incomplete or otherwise incorrect. When placing an international wire transfer order, Customer may be responsible for entering certain information provided to Customer by Bank, which may include, but is not limited to, the applicable exchange rate and/or a contract number. Customer acknowledges and agrees that Bank will not be liable for any loss, liability or expense incurred as a result of a Customer error related to entry of such required information. Customer acknowledges

and agrees that, in accordance with Article 4A of the Uniform Commercial Code, Bank shall be entitled to rely upon the numbers supplied by Customer to identify banks, payees (beneficiaries) and other parties to the wire transfer, even if those numbers disagree or are inconsistent with the names of those parties as provided by Customer. Bank and any other receiving financial institution shall have no obligation to determine whether a name and number identify the same person or institution. Customer acknowledges that payment of an order or related instructions may be made by the payee's (beneficiary's) bank on the basis of an identifying or bank account number even if it identifies a person different from the named payee (beneficiary).

9. Payment; Authorization to Charge Account. Customer agrees to pay Bank the amount of each wire transfer received from Customer on the Business Day Bank executes said wire transfer or at such other time as Bank may determine. Bank will validate that sufficient funds are available in Customer's Account prior to a wire transfer being executed. Generally, if sufficient funds are not available in Customer's Account, the wire transfer will not be executed by Bank. Bank may, without prior notice or demand, obtain payment of the amount of each wire transfer by debiting the Account designated. In the event there are not sufficient funds available in the Account, Bank also reserves the right to debit any other Account that Customer maintains with Bank.

10. Wire Confirmation; Account Reconciliation. Customer may confirm the execution of a wire transfer via the Bank Internet System. Completed wire transfers will also be reflected in Customer's periodic Account statement. Customer acknowledges and agrees that Bank is not obligated to provide Customer with a separate advice or notice for each completed wire transfer. If Customer requests that Bank provide a special notice and Bank agrees to do so, Bank reserves the right to impose a Service Fee for such notice in accordance with the Cash Management Master Agreement.

11. Service Providers. Bank may use a service provider to perform, as Bank's agent, all or any portion of Bank's obligations under this Appendix. Customer may be required to direct wire transfers and other requests to said provider.

12. Bank Reliance; Authentication.

12.1 Bank shall be entitled to rely in good faith on communications it receives as being given or sent by an Authorized Representative and as being genuine and correct. Bank shall not be liable to Customer for the consequences of such reliance.

12.2 BANK MAY TAKE SUCH ADDITIONAL STEPS AND IMPLEMENT SUCH PROCEDURES AS IT MAY DEEM APPROPRIATE TO VERIFY THE AUTHENTICITY OF ANY WIRE TRANSFER. BANK MAY DELAY THE EXECUTION OF ANY WIRE TRANSFER PENDING COMPLETION OF A CALL-BACK, OR RECEIPT OF ANOTHER FORM OF VERIFICATION WHICH IS SATISFACTORY TO BANK. IF BANK IS UNABLE TO OBTAIN SATISFACTORY VERIFICATION, BANK, IN ITS SOLE DISCRETION, MAY REFUSE TO EXECUTE ANY WIRE TRANSFER. In no event shall Bank be liable for any delay in executing a wire transfer or for failure to execute a wire transfer due to the absence of satisfactory verification.

12.3 Bank may electronically record any telephone conversations between Bank personnel and Customer with respect to the Services, in accordance with applicable law.

12.4 Wire transfer transactions are subject to all the foregoing and all regulations governing electronic transactions, including but not limited to Article 4A of the Uniform Commercial Code.

13. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the Services and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.



APPENDIX V

TD POSITIVE PAY SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and applies to all TD Positive Pay Services (the "Services") made available to Customer by Bank. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict. In the event of inconsistency between a provision of this Appendix and the Uniform Commercial Code ("U.C.C.," as further defined below), the parties intend to modify the effect of the applicable U.C.C. provisions to the maximum extent permitted by law.

TERMS AND CONDITIONS

1. Definitions.

1.1 Statutory Definitions. Unless otherwise defined in this Appendix, words or phrases shall have the meanings set forth in the U.C.C. in effect from time to time under the laws of the State specified in the governing law provision of the parties' Cash Management Master Agreement.

1.2 Definitions.

"Authorized Account" means the Account(s) of Customer, maintained at Bank, to which the Services described herein will apply.

"Available Funds" means funds on deposit in an Authorized Account and available for withdrawal pursuant to Federal Reserve Board Regulation CC and Bank's applicable funds availability schedule and policies.

"Check Issue File" means a record describing checks drawn by Customer on an Authorized Account and provided by Customer to Bank in accordance with Section 2.2.

"Exception Check" means a Presented Check or a Systematic Override Check (described in Section 2.2.2 below) that does not match data included in a Check Issue File.

"Exception Check Report" means a record describing Exception Checks which is provided by Bank to Customer in accordance with Section 2.3.

"Pay Decision(s)" means the instructions of Customer to Bank instructing Bank to pay an Exception Check.

"Presented Check" means a check, substitute check, or electronically-presented check drawn on an Authorized Account and presented to Bank for payment through the check collection system or over-the-counter at one of Bank's branch teller stations.

"Return Decision(s)" means the instructions of Customer to Bank instructing Bank not to pay an Exception Check.

"U.C.C." means the Uniform Commercial Code as in effect under the laws of the State specified in the parties' Cash Management Master Agreement, as it may be amended from time to time.

2. Services.

2.1 Description.

2.1.1 The Services described in this Appendix will provide Customer with a means to either affirmatively approve the payment of a particular check upon presentment or to object to its payment. Customer acknowledges that the Services have been identified by Bank as reducing the risk of fraudulent items being paid against Customer's Account(s) when such Services are adopted and properly utilized by Customer. By conforming to the terms and conditions of this Appendix, Customer agrees and acknowledges that Customer may significantly reduce the possibility that fraudulent items will post to Customer's Account(s).

2.1.2 Customer acknowledges and agrees that the Services apply only to magnetic ink character recognition (MICR) encoded paper checks and documents. Therefore, the Services and this Appendix shall not apply to any electronic funds transfer (EFT), Automated Clearing House (ACH) transaction, or check that has been converted to an ACH transaction that does not contain a serial number. Accordingly, this Appendix shall have no effect with respect to any such transactions on Bank or Customer's respective rights, obligations, duties or responsibilities under any other agreement between the parties or applicable law or regulation.

2.2 Check Issue File.

2.2.1 Customer shall submit a Check Issue File to Bank. The Check Issue File shall accurately state the check number and the exact amount of each check drawn on each Authorized Account since the last Check Issue File was submitted (and the payee name, if Customer elects to receive payee verification services

described below). Each Check Issue File shall also identify any checks that have been cancelled by Customer prior to issuance.

2.2.2 Payee Verification Services.

If Customer elects to receive payee verification services in conjunction with the Services, the following additional terms shall also apply. Bank's payee verification services require the payee name to match against Customer's Check Issue File at a minimum threshold or matching score. The payee name in the Check Issue File will be electronically compared to the payee name on Presented Checks. Other information related to the payee name may also be electronically compared as part of the automated verification process to establish a matching score. Such comparisons that result in a minimum threshold or matching score will be deemed to be a matching check. Customer is responsible for complying with the payee verification services' check specifications as specified by Bank from time to time in order to ensure the highest level of performance from the payee verification services. If Customer is unable or unwilling to comply with the payee verification services' check specifications as specified by Bank, Bank may, in its sole and exclusive discretion: (a) terminate or suspend Customer's use of the payee verification services as provided in the Cash Management Master Agreement, or (b) at Customer's request, re-configure the software associated with the payee verification services to systematically process Presented Checks in reliance solely on the payee name provided by Customer to Bank in the Check Issue File and without regard to any other information related to the payee name that may appear on the Presented Checks (hereinafter "Systematic Override Checks"). Any Presented Check or Systematic Override Check that does not result in a minimum threshold or matching score shall be deemed an Exception Check and reported as such in accordance with the terms of this Appendix. Except as may otherwise be provided in this Appendix and in the Cash Management Master Agreement, Bank shall have no liability for Systematic Override Checks.

2.2.3 Customer shall send the Check Issue File to Bank in the format and medium, by the deadline(s), at scheduled day(s), at the place(s) specified by Bank and agreed to by Customer, as set forth in Services' Setup Form(s). The deadline for transmissions of the Check Issue File to Bank shall be set forth in the Services' Setup Form(s).

2.3 Payment of Presented Checks and Reporting of Exception Checks.

2.3.1 Bank shall compare each Presented Check by check number, check amount and payee name (if Customer elects to receive payee verification services) against each Check Issue File received by Bank. Bank may satisfy its obligation hereunder by comparing check number, amount and payee name (if applicable) set forth in Substitute Checks, checks presented over-the-counter at one of Bank's teller stations and/or electronic presentment of checks. On each Business Day, Bank:

(a) may pay and charge to the Authorized Account each Presented Check that matches, by check number, amount and payee name (if applicable), a check shown in any Check Issue File;

(b) may pay and charge to the Authorized Account all Systematic Override Checks that match, by check number, amount and payee name (if applicable and as described herein), a check shown on any Check Issue File; and

(c) shall provide to Customer an Exception Check Report that indicates whether Bank has received any Exception Checks and, if so, provide the image of the Exception Check(s) by the deadline set forth in the Services' Setup Form(s) via the Bank Internet System. Customer must provide check payment approval or return instructions to Bank on each Exception Check reported by the deadline set forth in the Services' Setup Form(s) via the Bank Internet System ("Pay or Return Decisions").

2.3.2 Bank shall not pay any Presented Check for which Bank has received from Customer a stop payment request consistent with the terms and conditions of the parties' eTreasury Services Appendix or the Account Agreement.

2.4 **Payment and Dishonor of Exception Checks.** Except as provided in Section 2.4.4 below, Bank will pay or return Exception Checks in accordance with Customer's Pay or Return Decisions.

2.4.1 **Pay Decisions.** Bank shall finally pay and charge to the Authorized Account, to the extent there are sufficient Available Funds in the Authorized Account, any Exception Check that Customer directs Bank to pay.

2.4.2 **Return Requests.** Bank shall return to the depository bank any Exception Check drawn on an Authorized Account that Customer directs Bank to return.

2.4.3 **Default Options.** If Customer fails to provide Pay or Return Decisions to Bank in accordance with these requirements, Exception Checks will be handled in accordance with the default option as set forth in the Services' Setup Form(s) for each Authorized Account, in accordance with the following:

(a) **Return Default.** Where Customer has agreed to the return default option, Bank shall return to the depository bank any Exception Check drawn on that Authorized Account.

(b) **Pay Default.** Where Customer has agreed to the pay default option, Bank may finally pay and charge to the Authorized Account any Exception Check drawn on that Authorized Account.

2.4.4 Checks Presented for Payment at Bank Teller Stations.

2.4.4.1 Notwithstanding anything in this Appendix to the contrary, Bank may, in its sole and absolute discretion, return to the person presenting a check drawn on an Authorized Account for payment over-the-counter at one of Bank's teller stations any such check that does not appear on a Check Issue File (i.e., an Exception Check). Customer acknowledges and agrees that Bank shall

have no obligation to inform Customer that any such check has been presented for payment at a Bank teller station. Bank shall have no liability to Customer for wrongful dishonor with respect to any such check.

2.4.4.2 If a check drawn on an Authorized Account is presented for payment over-the-counter during such time the Bank is experiencing an interruption or failure of communications or data processing facilities or systems, emergency conditions, or any other difficulties beyond the control of Bank, then, notwithstanding any other provision of this Appendix, Customer authorizes Bank to pay the Presented Check, even if the Presented Check is an Exception Check. Additionally, Bank shall have no obligation to notify Customer of any such Presented Check.

2.5 Customer and Bank Communications.

2.5.1 Customer or Bank, at its discretion, may each submit to the other party a revision of any communication provided for under this Appendix (e.g., the revision of Check Issue Files, Exception Check Reports, Pay Decisions, Return Decisions). The revised communication must (i) be sent in its entirety and not in the form of a partial amendment to the communication originally sent, (ii) identify the original communication, and (iii) be sent in the format and medium, by the deadline(s), and at the place(s) established by the receiving party. A properly submitted revised communication serves to revoke the original communication.

2.5.2 Bank shall use only Check Issue Files that comply with Section 2.2 and have not been revoked in accordance with Section 2.5.1 in the preparation of Exception Check Reports under this Appendix.

2.5.3 Customer shall use only Exception Check Reports that comply with Section 2.3 and have not been revoked in accordance with Section 2.5.1 in the preparation of Pay Decisions and Return Decisions. Bank shall not be obligated to comply with any Pay Decision or Return Decision received in a format or medium, after a deadline, or at a place not permitted under this Appendix and Services' Setup Form(s), but may instead treat such a Pay Decision or Return Decision in accordance with the default option agreed to by Customer in the Services' Setup Form(s).

2.5.4 Bank is not responsible for detecting any Customer error contained in any Check Issue File, Pay Decision or Return Decision sent by Customer to Bank.

2.6 **Submission of Data Prior to Implementation of Services.** Customer shall submit to Bank a current, reconciled list of all outstanding checks issued on each Authorized Account one (1) week prior to the implementation of the Services hereunder. Depending on the frequency with which Customer issues checks, Bank reserves the right to require Customer to submit one or more additional such lists so that all outstanding, unpaid checks issued on any Authorized Account have been reported to Bank prior to the implementation of the Services.

3. Remedies.

3.1 **U.C.C. Liability.** To the extent applicable, the liability provisions of U.C.C. Articles 3 and 4 shall govern this Appendix, except as modified below. To the extent permitted by U.C.C. Articles 3 and 4, the liability of Bank under this Appendix shall in all cases be subject to the provisions of the parties' Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank.

3.2 **Wrongful Honor.** It shall constitute wrongful honor by Bank if Bank pays an Exception Check listed in a timely Exception Check Report unless: (i) Customer issued a Pay Decision, or (ii) Customer agreed to the pay default option and did not issue a Return Decision by the deadline set forth in the Services' Setup Form(s). In the event that there is wrongful honor, the following shall apply:

3.2.1 Bank shall be liable to Customer for the lesser of the amount of the wrongfully paid Exception Check or Customer's actual damages resulting from Bank's payment of the Exception Check.

3.2.2 Bank expressly waives any right it may have to assert that Customer is liable for the amount of the wrongfully honored Exception Check on the grounds that the Exception Check was properly payable under U.C.C. Section 4-401.

3.2.3 Bank retains the right to assert Customer's failure to exercise reasonable care under U.C.C. Sections 3-406 and 4-406.

3.2.4 Bank retains the right to assert the defense that Customer has sustained no actual damages because Bank's honor of the Exception Check discharged for value an indebtedness of Customer.

3.3 **Wrongful Dishonor.** Except as provided below, it shall constitute wrongful dishonor by Bank if Bank dishonors an Exception Check: (i) that Bank has been ordered to pay pursuant to a Pay Decision, or (ii) for which Customer has not issued a Return Decision under the pay default option by the deadline set forth in the Services' Setup Form(s).

3.3.1 Bank's liability for wrongful dishonor of an Exception Check shall be limited to the damages for wrongful dishonor recoverable under U.C.C. Articles 3 and 4.

3.3.2 Notwithstanding Section 3.3.1, Bank shall have no liability to Customer for wrongful dishonor when Bank, acting in good faith, returns an Exception Check:

(a) that it reasonably believed was not properly payable; or

(b) if there are insufficient Available Funds on deposit in the Authorized Account; or

(c) if required to do so by the service of legal process on Bank or the instructions of regulatory or government authorities or courts.

3.4 Rightful Payment and Dishonor. Except as provided in Section 3.5, the following shall apply:

3.4.1 If Bank honors an Exception Check in accordance with the pay default option agreed to Customer or in accordance with a Pay Decision issued by Customer, such honor shall be rightful, and Customer waives any right it may have to assert that the Exception Check was not properly payable under U.C.C. section 4-401.

3.4.2 If Bank dishonors an Exception Check in accordance with the return default option agreed to by Customer or in accordance with a Return Decision issued by Customer, the dishonor shall be rightful, and Customer waives any right it may have to assert that the dishonor was wrongful under the U.C.C. section 4-402.

3.4.3 Customer agrees that Bank exercises ordinary care whenever it rightfully pays or returns an Exception Check consistent with the provisions of this Appendix.

3.5 Faulty Information. Subject to the terms and conditions of the Cash Management Master Agreement, Bank shall be liable for losses, other than incidental or consequential damages, proximately caused by its honor of a check that was not properly payable, or its dishonor of a check that was properly payable, if the honor or dishonor occurred because Bank, in accordance with the provisions of Section 2 of this Appendix:

(a) should have shown the check on an Exception Check Report but failed to do so due to Bank error, unless Bank provided Customer with timely information that disclosed the error; or

(b) showed the check on an Exception Check Report but referenced the wrong check number due to Bank error, unless Bank provided Customer with timely information that disclosed the error.

3.6 Assignment. To the extent that Customer suffers a loss under this Appendix, Bank assigns to Customer any claim that Bank would have against a depository or collecting bank to recover the loss, including any claim of breach of warranty under U.C.C. Sections 4-207, 4-208, and 4-209.

4. Stop Payment and Return Decisions. The Services will not be used as a substitute for Bank's stop payment services. Customer will follow Bank's standard stop payment procedures if it desires to return a check that matches the data included in a Check Issue File or other check that was validly issued. Nothing in this Appendix will limit Customer's right to stop payment on any check that matches the data included in a Check Issue File or other check, or Bank's right to return any check that matches the data included in a Check Issue File or other check that Customer has authorized Bank to pay in accordance with this Appendix if Bank determines in its sole discretion that the check is not properly payable for any reason (without Bank's agreeing to, or being required to, make such determination in any circumstance) or that there are insufficient collected or Available Funds in the Authorized Account to pay it.

5. Governing Law. Except where expressly required by contrary provisions of the U.C.C., any claim, controversy or dispute arising under or related to this Appendix shall be governed by and interpreted in accordance with the governing law provision of the parties' Cash Management Master Agreement.

6. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the Services and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the parties' Cash Management Master Agreement is terminated. In the event of termination, all sums owed to Bank hereunder shall be immediately due and payable.



APPENDIX VIII

TD DIGITAL EXPRESS SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and applies to all TD Digital Express Services (the "Services") made available to Customer by Bank. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. **Services.** The Services provide Customer with an Internet-based system designed to expedite check depositing services by enabling Customer to use check conversion technology to submit to Bank, for deposit to Customer's Account(s), electronic check images and associated information ("Check Images") in lieu of the original checks from which such Check Images were obtained. These Services are provided in accordance with the *Check Clearing for the 21st Century Act* ("Check 21").

2. Hardware Requirements.

2.1 In order to use the Services, Customer must utilize certain Bank-approved image/scanner hardware (the "Hardware"). Customer must either (a) have or obtain the Hardware, as approved by Bank ("Customer Hardware"), or (b) utilize Hardware provided by Bank ("Bank Hardware"). Customer must also have a Computer as outlined in the Cash Management Master Agreement, as Bank may specify and approve from time to time.

2.2 If Customer elects option (a), Customer Hardware, Customer is solely responsible for the purchase, maintenance, performance and adequacy of Customer Hardware. Bank makes no representations or warranties concerning, and has no responsibility or liability for, Customer Hardware or its use with the Services. Bank shall have no liability or responsibility whatsoever for errors, including but not limited to processing or transmission errors, resulting from any Check Images transmitted by Customer using Customer Hardware.

2.3 If Customer elects option (b), Bank Hardware, Customer agrees as follows:

(i) Bank will retain ownership of Bank Hardware provided by Bank for use with the Services.

(ii) Customer will not use Bank Hardware in connection with any remote check deposit service offered by any other financial institution other than Bank.

(iii) Customer acknowledges that Bank did not manufacture Bank Hardware and has provided the same to Customer on an "AS IS" basis, and warrants only that, upon delivery, Bank Hardware will conform to Bank's then current applicable standards for use of the Services. Bank Hardware is provided to Customer with a standard

manufacturer's warranty. Customer shall thereafter be responsible for purchasing any and all additional manufacturer warranty period(s) beyond the standard warranty, as may be made available by the manufacturer, for complying with all manufacturer recommendations for preventive maintenance, or for repairing or replacing Bank Hardware.

(iv) Customer shall bear the entire risk of loss, theft, damage or destruction of Bank Hardware from the date of receipt until return shipment to a Bank branch or shipped postage-paid to Bank. Such loss, damage or destruction of Bank Hardware shall not relieve Customer of the obligation to make payments or to comply with any other obligation under this Appendix.

(v) Upon termination of this Appendix by either party for any reason, Customer shall return Bank Hardware in the same condition as when originally provided to Customer, except for ordinary wear and tear resulting from proper use. Bank Hardware shall be packed for proper return shipment to such place as Bank shall specify. In the event Bank Hardware has not been returned within fifteen (15) Business Days of termination of this Appendix, Customer shall make payment to Bank in an amount equivalent to the depreciated value for Bank Hardware. Where agreed to by Bank in its sole discretion, Customer may purchase Bank Hardware from Bank, subject to the terms and conditions of Bank's bill of sale or similar agreement.

3. Check Images; Image Replacement Documents.

3.1 Customer may use the Services to deposit original paper checks using the Hardware to scan, capture and submit Check Images to Bank through the Services' Internet site ("Services Site"). Eligible items for deposit include original checks that Customer has received for payment or deposit, and obligations of financial institutions (travelers' checks, cashier checks, official checks, and money orders).

3.1.1 The following check types are *not eligible* for use with and may not be processed using the Services:

- (i) Checks drawn on banking institutions outside the U.S. or in currencies other than U.S. Dollars;
- (ii) Irregular checks (e.g., where the numerical and written amounts are different);

- (iii) Previously-returned checks;
- (iv) Checks payable to or in cash;
- (v) Checks exceeding any Customer transaction or file limits as Bank may establish from time to time; and
- (vi) Checks that are postdated or more than six (6) months old.

3.1.2 The following check types are *restricted* for use with and may only be processed using the Services with prior approval by Bank (as further described below):

- (i) Checks payable to a third party (rather than to Customer) (hereinafter "Third Party Checks"); and
- (ii) Remotely-created checks (or remotely created payment orders deposited into or cleared through the check clearing system) (hereinafter, collectively referred to simply as "remotely-created checks" unless otherwise expressly specified).

Notwithstanding the foregoing, under no circumstances may Customer use the Services to deposit any check types that Customer is banned or prohibited from using or accepting under applicable law, including, by way of example only, the use or acceptance by sellers and telemarketers of remotely created payment orders (which include remotely-created checks) as defined and described in the Federal Trade Commission's Telemarketing Sales Rule.

3.2 Third Party Checks. Customer shall request approval from Bank prior to any use of the Services to process Third Party Checks, which permission Bank may grant or refuse in its sole and exclusive discretion. Such use of the Services and the scope of permitted Third Party Checks may be limited or restricted by Bank in its sole and exclusive discretion, including without limitation to those Third Party Checks that have been properly endorsed over to Customer as further described below.

3.2.1 If approved to use the Services to process Third Party Checks, Customer shall make the following additional representations and warranties upon each delivery to Bank of an Electronic File (as defined below) containing Third Party Checks:

- (i) All endorsement(s) on the original Third Party Checks are legible, genuine and accurate;
- (ii) Customer has instituted procedures to ensure that each original Third Party Check was authorized by the drawer in the amount stated on the original Third Party Check and to the payee(s) stated on the original Third Party Check;
- (iii) Each Third Party Check contains all endorsements applied by the prior payee(s) stated on the original Third Party Check and has been properly endorsed by such payee(s) for payment over to Customer;
- (iv) Customer is authorized to enforce each Third Party Check that is transmitted to Bank using the Services, and Customer is authorized to obtain payment of and each

Third Party Check is properly payable to and enforceable by Customer; and

Consistent with the terms of this Appendix as well as the Account Agreement, if a Third Party Check is returned, Customer owes Bank the amount of the Third Party Check, regardless of when the Third Party Check is returned. Bank may withdraw funds from Customer's Account to pay the amount owed to Bank, and if there are insufficient funds in Customer's Account, Customer will owe the remaining balance.

Except where otherwise provided, all other provisions of this Appendix shall apply to Third Party Checks and to Customer's use of the Services in conjunction with Third Party Checks.

3.3 Remotely-Created Checks. A remotely-created check, unlike a typical check or draft, is not created by the paying or drawer bank and does not contain the signature of the account-holder (or a signature purporting to be the signature of the account-holder). In place of a signature, the check generally has a statement that the account-holder authorized the check or has the account-holder's name typed or printed on the signature line. Customer shall request approval from Bank prior to any use of the Services to process remotely-created checks, which permission Bank may grant or refuse in its sole and exclusive discretion. Such use of the Services and the scope of permitted remotely-created checks may be limited or restricted by Bank in its sole and exclusive discretion, and/or by applicable law.

3.3.1 If approved to use the Services to process remotely-created checks, Customer shall be deemed to make the following additional representations and warranties upon each delivery to Bank of an Electronic File containing remotely-created checks:

- (i) Customer has received express and verifiable authorization to create the check in the amount and to the payee that appears on the check;
- (ii) Customer will maintain proof of the authorization for at least two (2) years from the date of the authorization, and supply Bank with such proof, if Bank requests it, within five (5) Business Days of the request; and
- (iii) Consistent with the terms of this Appendix as well as the Account Agreement, if a remotely-created check is returned, Customer owes Bank the amount of the check, regardless of when the check is returned. Bank may withdraw funds from Customer's Account to pay the amount owed to Bank, and if there are insufficient funds in Customer's Account, Customer will owe the remaining balance.

All other provisions of this Appendix shall apply to remotely-created checks and to Customer's use of the Services in conjunction with remotely-created checks.

3.3.2 Each of Bank and Customer agrees to operate in accordance with applicable laws and regulations regarding remotely-created checks, including

but not limited to, Regulation CC and applicable warranties, the Uniform Commercial Code and applicable warranties, the Bank Secrecy Act, USA Patriot Act, and the Federal Trade Commission Telemarketing Sales Rule, as the same may be amended from time to time. Without limiting the foregoing, Customer represents, warrants and covenants that it will not use the Services to deposit any check types that Customer is banned or prohibited from using or accepting under applicable law.

3.4 If at any time Bank believes that Customer's use of the Services to deposit Third Party Checks and/or remotely-created checks may create a risk of financial loss or otherwise result in unacceptable exposure to Bank, including but not limited to unacceptable rates of returned items, or may be subject to or otherwise involve irregular, unauthorized, fraudulent or illegal activity, Bank may, at its sole discretion, immediately and without prior notice to Customer, suspend or terminate Customer's use of the Services, and/or Customer's use in conjunction with Third Party Checks and/or remotely-created checks, in addition to but not in lieu of all other rights and remedies available to Bank under this Appendix and the Agreement. Bank shall provide prompt subsequent notice to Customer of any such suspension or termination of Customer's use of the Service.

3.5 Customer shall enter check information into the Services Site, imaging the front and the back of each paper check and capturing the information contained in the MICR line of the paper check. Customer shall review each Check Image for clarity to ensure that the item is legible and can be reproduced as an Image Replacement Document ("IRD(s)" or "Substitute Check(s)"). Using the Services, an electronic file will be created ("Electronic File") that contains electronic information relating to and converted from the paper checks that have otherwise been truncated or removed from the forward collection and payment process (each an "Electronic Item"). To ensure accuracy, Customer shall balance the dollar total of each deposit to the sum of the Electronic Items prior to transmitting the Electronic File to Bank.

3.6 Customer authorizes and agrees that Bank may, in conjunction with and via the Services, add the image of an endorsement, an electronic endorsement or a "virtual endorsement" for Customer to the Check Image of any check or item deposited under the terms of this Appendix, and that such endorsement shall be legally enforceable against Customer even though the endorsement did not appear and was not placed on the original paper check or item. In the event Bank does supply a virtual or similar endorsement, Bank may instruct Customer not to otherwise endorse the check or item so as to minimize any conflict with the legibility of the virtual endorsement.

3.7 Customer shall determine that the Electronic File has been received based on the confirmation page of the Services Site. Bank will indicate acceptance of the transactions and any transactions rejected by the Services on the Services Site. Customer shall process any rejected transactions as paper checks through the normal paper check deposit process.

3.8 Customer shall enter the dollar amount of a paper check(s), along with any other optional information that Customer would like retained by the Services Site. The Services Site provides for reports and exporting of the information that has been entered.

3.9 Bank shall electronically deliver to Customer, through the Services Site, a confirmation of receipt for each deposit submitted, and the deposit shall be considered received by Bank when such confirmation is delivered to Customer. Deposits received via the Service by 9:00 p.m. Eastern Time on any Business Day or at any time on any Calendar Day that is not a Business Day will be posted to Customer's Account on the same Business Day, with next Business Day availability of deposits based on Bank's Account Agreement. Bank reserves the right to reject any single Check Image or group of Check Images for any reason, before or after delivery of confirmation of receipt.

3.10 Customer acknowledges and agrees that in the event any deposited item converted to a Check Image is returned for any reason (for example, non-sufficient funds), Bank may return the item to Customer by delivery of either a Substitute Check or the Check Image, including all return information. Return items will be handled in the same manner as check deposits in accordance with the Account Agreement.

4. Customer Responsibilities and Obligations.

4.1 Customer represents, warrants and covenants that after truncation of an original check, Customer shall safeguard the Electronic Items and original checks identified in any Electronic File previously sent to Bank in order to ensure that such original checks and Electronic Items: (i) shall not be submitted for deposit with Bank or any other financial institution, except in accordance with the terms and conditions of this Appendix related to unprocessable Electronic Items and (ii) shall not be transferred for value to any other person or other entity. As an additional security control, Customer shall ensure that the front of each original check is properly marked with wording or other marking in order to reflect that the deposit has been sent for processing.

4.2 Upon receipt of any transmitted Electronic File, Bank shall be the lawful owner of such Electronic File and each Electronic Item with respect to original checks imaged in that Electronic File. Customer shall retain all original checks truncated pursuant to this Appendix for a period of thirty (30) Calendar Days in a manner that is mutually agreed upon between the parties hereto. However, for accounting, auditing and other legal purposes, Customer may keep electronic records regarding its receipt and deposit of such checks, provided such internal electronic records cannot be used to generate duplicate Electronic Files for purposes of depositing and presenting such checks for payment.

4.3 Customer shall deliver promptly to Bank, upon its request, the original check if a request is made within the retention period provided above, or Substitute

Check or Sufficient Copy thereof, for each Electronic Item created by Customer. The term "Sufficient Copy" means a copy of an original check that accurately represents all of the information on the front and back of the original check as of the time the original check was truncated or is otherwise sufficient to determine whether or not a claim is valid.

4.4 Customer shall not create at any time an Electronic File under this Appendix or otherwise use the Services to capture or maintain tax identification numbers or non-public personal information of any third-party from whom Customer has received an original check for payment or deposit or which Customer has selected for truncation.

4.5 Customer agrees to abide by all federal and state laws, and rules and regulations applicable to a customer of the banking transactions described in this Appendix.

4.6 If Bank receives a returned item for a check deposited by Customer after Customer has terminated this Appendix, then Customer agrees that Bank may debit Customer's Account, or if such Account has been closed by Customer, Bank will send a request for payment to Customer, and Customer agrees to pay Bank within a commercially reasonable period of time.

4.7 Customer agrees to have controls in place to ensure that the Services, including the Hardware and checks processed through the Hardware, are properly safeguarded and stored in accordance with the timeframe set forth in Section 4.2 above and in a secure location, under effective control, in order to safeguard against unauthorized access and use. Customer shall ensure that all such checks are thereafter destroyed by a cross-shredder, and/or pulped or otherwise destroyed in such a manner that does not permit recovery, reconstruction or future use of the checks. Customer agrees that it will not simply throw out such paper checks with other classes of records or with miscellaneous trash. Customer agrees to be responsible for all damages resulting from lack of proper controls over processed checks.

4.8 Customer shall notify Bank of any interruptions in, delay or unavailability of, or errors caused by the Services immediately upon discovery thereof. Notwithstanding the foregoing, in the case of any error caused by the Services and subject to Section 11 of the parties' Cash Management Master Agreement, Customer shall provide such notice within thirty (30) Calendar Days of the date of the earliest notice to Customer which reflects the error. Failure of Customer to provide such notice to Bank shall relieve Bank of any liability or responsibility for such error, omission or discrepancy.

5. Customer Warranties, Covenants. Customer makes the following representations, warranties and covenants as of the effective date of this Appendix and upon each delivery of an Electronic File to Bank:

5.1 An Electronic File may include an electronic representation of a Substitute Check. Customer shall redeposit a returned original check or a returned Electronic Item by delivering the same to any Bank branch location. A returned original check or returned Electronic Item may not be re-submitted by Customer using the Services. Customer may only use the Services to re-submit

an IRD or Substitute Check that has been returned to Customer for non-sufficient funds.

5.2 With respect to each Electronic Item in any Electronic File delivered to Bank, the Electronic Item accurately represents all of the information on the front and back of the original check as of the time that the original check was created by the payor; contains all required and valid endorsements; replicates the MICR line of the original check; and meets all FRB standards of and technical requirements for sending Electronic Items to any as set forth in the applicable FRB operating circular, or as established by the American National Standards Institute ("ANSI") or any other regulatory agency, clearing house or association. Specifically, each Electronic Item of each original check shall be of such quality that the following information can clearly be read and understood by sight review of such Electronic Item:

- (i) the amount of the check;
- (ii) the payee of the check;
- (iii) the signature of the payor of the check;
- (iv) the date of the check;
- (v) the check number;
- (vi) the information identifying the payor and the paying bank that is preprinted on the check, including the MICR line; and
- (vii) all other information placed on the original check prior to the time an image of the original check is captured, such as any required identification written on the front of the check and any endorsements applied to the back of the check.

5.3 Customer shall also ensure that the following information is captured from the MICR line of each original check:

- (i) the American Bankers Association routing transit number ("RTN");
- (ii) the number of the account on which the check is drawn;
- (iii) when encoded, the amount of the check; and
- (iv) when encoded, the auxiliary on-us field (serial number) and the process control field of the check.

5.4 The Electronic Item bears all endorsements, if any, applied by previous parties that handled the check in any form (including the original check, as Substitute Check, or another paper or electronic representation of such original check or Substitute Check) for transfer, forward collection or return.

5.5 Customer is entitled to enforce the original check, or Customer is authorized to obtain payment of the original check on behalf of a person who is either entitled to enforce the original check or is authorized to obtain payment on behalf of a person entitled to enforce the original check.

5.6 Customer will submit financial and/or other additional information to Bank upon request in order for Bank to establish or amend Customer's deposit and file limits as further described in Section 6 and as established by Bank and communicated to Customer, or to otherwise monitor or audit Customer's use of the Services and compliance with this Appendix. Customer will also notify Bank of any change in transaction volumes or financial condition that may have an effect on this Appendix or Customer's use of the Services.

5.7 Customer shall also request permission from Bank in advance of any change in locations at which the Services are used or change in the physical location or address of any Hardware from its original Bank-approved location or address, which permission Bank may not unreasonably withhold provided that the new physical location or address remains within the continental United States and in those states in which Bank operates from time to time. In addition to but not in lieu of the foregoing, Customer shall request advance permission from Bank prior to using the Services and/or any Hardware outside the continental United States and/or outside of those states (including the District of Columbia) in which Bank operates from time to time. Bank may grant or decline such request in its sole and exclusive discretion and in consideration of applicable law.

5.8 Both Customer and the clients with whom it does business are reputable and are not using Bank as a conduit for money laundering or other illicit purposes.

5.9 None of Customer's authorized transactions to be processed by Bank are prohibited by any applicable federal or state law, regulation, order, rule or judgment.

5.10 Customer Electronic Files will not contain viruses that originate from Customer's Computer, in accordance with the requirements of Section 7 of the Cash Management Master Agreement.

5.11 None of Customer's employees are a national of a designated blocked country or "Specially Designated National", "Blocked Entity", "Specially Designated Terrorist", "Specially Designated Narcotics Trafficker", or "Foreign Terrorist Organizations" as defined by the United States Office of Foreign Assets Control.

5.12 Customer is responsible for implementing operational controls and risk-monitoring processes, as well as conducting periodic self-assessments of the security of the Services and its processes and practices with regard to use of the Services.

6. Deposit and File Limits. Customer's use of the Services is limited as more particularly described in the Services' Setup Form(s), and as the parties may otherwise agree from time to time. Such limits may include but are not limited to, e.g., maximum total daily dollar amounts; maximum per item dollar amounts; maximum percentage of monthly transactions returned; and maximum number of items to be deposited per day.

7. Administrator(s) and Authorized Users.

7.1 Customer may designate Administrator(s) relative to the Services, as set forth in the Services' Setup Form(s). Customer is solely responsible for designating its Administrator(s). Customer agrees to provide Bank, upon Bank's request, with any certificate or documentation that is acceptable to Bank specifying the name of the person who is authorized to be designated as Administrator(s) from time to time.

7.2 The Administrator(s) may designate other Administrators and/or Authorized Users. Customer accepts as its sole responsibility an Administrator's designation of other Administrators and Authorized Users. Customer understands that the Administrator(s) will control, and Customer authorizes the Administrator(s) to control, access by other Administrator(s) and Authorized Users of the Services through the issuance of passwords. The Administrator(s) may add, change or terminate Customer's Authorized Users from time to time and in his/her sole discretion. Bank does not control access by any of Customer's Authorized Users to any of the Services.

7.3 Customer will require each Administrator and each Authorized User to comply with all provisions of this Appendix and all other applicable agreements. Customer acknowledges and agrees that it is fully responsible for the failure of any Administrator or any Authorized User to so comply.

7.4 Whenever any Authorized User leaves Customer's employ or Customer otherwise revokes the authority of any Authorized User to access or use the Services, Customer must notify the Administrator immediately, and the Administrator is solely responsible for de-activating such Authorized User's password. Whenever an Administrator leaves Customer's employ or Customer otherwise revoke an Administrator's authority to access or use the Services, Customer remains fully responsible for all use of the passwords and the Services.

8. Security Procedures.

8.1 Upon successful enrollment, Customer can access the Services via the Services Site, or any website that Bank may designate from time to time, using the security procedures as described from time to time. Bank will provide Customer with an organizational or User ID that is the electronic identification, in letters and numerals, assigned to Customer by Bank that will be used for log-in by Customer's Administrator(s) and Authorized User(s). Bank will also provide the Administrator(s) initially designated by Customer with an initial individual password to gain access to the Services. The Administrator(s) and Authorized User(s) must change his or her individual password from time to time for security purposes, as prompted by the Services Site, or more frequently.

8.2 Customer acknowledges that Administrator(s) will, and Customer authorizes Administrator(s) to, select other Administrators and Authorized Users by issuing to any person an individual password. Customer further acknowledges that Administrator(s) may, and Customer authorizes

Administrator(s) to, change or de-activate the individual password and/or any individual password from time to time and in his or her sole discretion.

8.3 Customer acknowledges that, in addition to the above individual passwords, access to the Services includes, as part of the Access Devices, a multi-factor authentication security procedure at log-in for Customer, including Administrator(s) and Authorized Users. This additional security procedure involves an additional access code and Computer registration that is in addition to User ID and individual password security (hereinafter "Enhanced Log-in Security").

8.4 Bank does recommend as a commercially reasonable security procedure that Customer implement dual control of the Services, whereby one Authorized User creates, edits, cancels, deletes and restores an Electronic File, and a second different Authorized User reviews the Electronic File prior to it being released.

8.5 Customer accepts as its sole responsibility the selection, use, protection and maintenance of confidentiality of, and access to, the Access Devices. Customer agrees to take reasonable precautions to safeguard the Access Devices and keep them confidential. Customer agrees not to reveal the Access Devices to any unauthorized person. Customer further agrees to notify Bank immediately if Customer believes that the confidentiality of the Access Devices has been compromised in any manner.

8.6 The Access Devices identify and authenticate Customer (including Administrator(s) and Authorized Users) to Bank when Customer accesses or uses the Services. Customer authorizes Bank to rely on the Access Devices to identify Customer when Customer accesses or uses any of the Services, and as signature authorization for any transaction, transfer or other use of the Services. Customer acknowledges and agrees that Bank is authorized to act on any and all communications or instructions received using the Access Devices, regardless of whether the communications or instructions are authorized. Bank owns the Access Devices, and Customer may not transfer them to any other person or entity. If this Appendix is terminated, Customer's access to the Services will be immediately terminated.

8.7 Customer acknowledges and agrees that the Access Devices and other security procedures applicable to Customer's use of the Services are a commercially reasonable method for the purpose of verifying whether any transaction, transfer or other use of the Services was initiated by Customer. Customer agrees to be responsible for any transmission Bank receives through the Services that is processed by Bank in accordance with the security procedures, even if such transmission is not authorized by Customer, including any fraudulent transmission by Customer's employees or agents. Customer agrees that any election Customer may make to change or waive any optional security procedures recommended by Bank is at Customer's risk and that any loss resulting in whole or in part from such change or waiver will be Customer's responsibility. Customer further acknowledges and agrees

that the Access Devices are not intended, and that it is commercially reasonable that the Access Devices are not intended, to detect any errors relating to or arising out of a transaction, transfer or any other use of the Services.

8.8 If Customer has reason to believe that any Access Devices have been lost, stolen or used (or may be used) or that a transaction, transfer or other use of the Services has been or may be made with any Access Devices without Customer's permission, Customer must contact its Administrator. Customer also agrees to provide Bank with immediate notice of any actual or suspected breach in the security of or other unauthorized access to the Services through use of Customer's Computer. Such notice shall include a description of the incident in general terms; a description of the type of information or data related thereto that was the subject of unauthorized access or use; a description of what Customer has done to protect the information or data from further unauthorized access; and a telephone number or other contact information so that Bank can call for further information or inquiry. In no event will Bank be liable for any unauthorized transaction(s) that occurs with any Access Devices, where such communications or instructions were provided to Bank in accordance with the security procedures and other terms as set forth in the Cash Management Master Agreement, except for any damages resulting from any acts or omissions of Bank.

9. **Limitation of Liability.** In addition to but not in lieu of the limitations of liability and related provisions contained in the parties' Cash Management Master Agreement, Bank shall have no liability for any error or delay in performing the Services and shall have no liability for not affecting a Check Image, if:

(i) Bank receives actual notice or has reasonable belief that Customer has filed or commenced a petition or proceeding for relief under any bankruptcy or similar law;

(ii) The ownership of funds involving a Check Image or Customer's authorized representative's authority to transmit a Check Image is in question;

(iii) Bank reasonably suspects a breach of the security procedures;

(iv) Bank reasonably suspects that Customer's Account has been used for illegal or fraudulent purposes; or

(v) Bank reasonably believes that a Check Image is prohibited by federal law or regulation, or otherwise so provided in the Appendix.

Further, Bank will not be liable to Customer for any unauthorized actions or fraud initiated or caused by Customer or its employees or agents. Bank will also be excused from failing to transmit or delay in transmitting a Check Image if such transmittal would result in it exceeding

any limitation imposed on it by any governmental or regulatory body.

10. Audit Rights and Site Visits; Internal Controls. Bank, its accountants, auditors or agents shall have the right to conduct site visits of Customer, as well as review, inspect and audit, at Bank's expense and with reasonable notice, and at any time as Bank may in good faith deem necessary or reasonable during or after the term of this Appendix, Customer's compliance with the terms of this Appendix, including but not limited to Customer's use of the Services, its Computer and security infrastructure, and the books and records of Customer related to: (i) Customer's activities hereunder and/or (ii) conformance with Customer's obligations hereunder. In addition, Bank reserves the right, in its sole and exclusive discretion, to require Customer to implement additional internal controls at Customer location(s) where use of the Services occurs and to request information from Customer relative to Customer's security infrastructure. Any review, inspection or audit to be performed by or for Bank pursuant to this Section 10 shall be conducted only during normal business hours, using reasonable care not to cause damage and not to interrupt the normal business operations of Customer.

11. Survival. The provisions of Section 9, as well as Customer's obligation to produce the original of, or a Sufficient Copy of, any item accepted within any deposit upon Bank's request in accordance with Section 4 hereof, and Customer's liability for breach of any representation and/or warranty made in Sections 3, 4 and 5 hereof shall survive termination of this Appendix and/or the Cash Management Master Agreement.

12. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the Services and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.



APPENDIX IX

TD ACCOUNT RECONCILEMENT SERVICES - FULL

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and applies to all TD Account Reconciliation Services – Full (the "Services") made available to Customer by Bank. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. Services. The Services described in this Appendix will assist Customer in reconciling and managing the check and deposit activity in Customer's designated checking Account(s) ("Authorized Accounts"). Use of the Services does not affect any of Customer's obligations, which are described in the Account Agreement, to discover and report unauthorized or missing signatures and endorsements, or alterations on checks drawn on Customer's Accounts.

2. Submission of Data.

2.1 Customer shall have its checks prepared in accordance with Bank specifications, and will supply Bank with twenty-five (25) voided checks to be used for testing. The checks will be tested to ensure the paper stock is of a minimum weight and is encoded with Bank's ABA (routing and transit) number, account number and check number to ensure the readability of the MICR line on Bank's equipment.

2.2 Customer shall send a file to Bank containing information regarding checks that have been issued by Customer ("Check Issue File") in the format and medium, by the scheduled day(s) and to the place(s) specified by Bank and agreed to by Customer as set forth in the Services' Setup Form(s). The Check Issue File shall include check issue date, check issue amount, payee, stop payments, and voided or cancelled checks, if applicable.

2.3 Prior to implementation of the Services, Customer shall submit to Bank a current, reconciled list of all outstanding checks issued on each Authorized Account one (1) week prior to the implementation of the Services hereunder. Depending on the frequency with which Customer issues checks, Bank reserves the right to require Customer to submit one or more additional lists so that all outstanding, unpaid checks issued on any Authorized Account have been reported to Bank prior to the implementation of the Services hereunder.

2.4 Customer will send to Bank a test file in the format and medium as identified in the Services' Setup

Form(s) to ensure the readability of the Check Issue File on Bank's equipment.

2.5 Customer agrees to receive its paid check data ("Paid Check Data") from Bank in the specified format and medium, on the scheduled day(s) and at the place(s) specified by Bank and as set forth in the Services' Setup Form(s).

2.6 Prior to receiving a file from Bank containing Customer's Paid Check Data, Customer will be provided with a test file by Bank to ensure the readability of the Paid Check Data, on Customer's equipment. Customer agrees to report any test file failures.

2.7 Bank shall compare each of Customer's paid checks by check number and amount against each Check Issue File received by Bank. Bank does not, and shall not be obligated to, compare any other data (such as payee names) on a presented check with a Check Issue File, even if a Check Issue File contains such other data. Bank may satisfy its obligation hereunder by comparing check numbers and amounts received in Substitute Checks (as defined in the Cash Management Master Agreement) and/or via electronic presentment of checks.

3. Statement of Transactions. Within five (5) Business Days following the scheduled date for reconciliation, as set forth in the Services' Setup Form(s), or receipt of the final Check Issue File for the current reconciliation period as set forth in the Services' Setup Form(s), Bank will provide a fully reconciled report including a listing in check number sequence of all outstanding paid, issued, voided, stopped and cancelled items from the statement schedule. Customer shall review the listing and report any errors as set forth in the Cash Management Master Agreement between Bank and Customer. Customer's use of the Services or Bank's receipt of information associated with the Services does not increase Bank's or Customer's duties or obligations with respect to Customer's Accounts.

4. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. Each of Bank's and Customer's liability under this Appendix shall in all cases be subject to the provisions of the Cash

Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to

the Services and shall remain in full force and effect until termination or such time as a different or amended Full Reconciliation Services Appendix is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.

Remainder of page intentionally left blank.



APPENDIX XIV

TD CURRENCY SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and applies to all TD Currency Services (the "Services") made available to Customer by Bank or Bank's third-party service provider. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. **Services.** The Services described in this Appendix provide Customer with (1) money room cash and check deposit processing, as described in further detail below, including: counting, validating, posting and adjustments to Customer's Account, and (2) cash disbursement orders, as described in further detail below, including: packaging of coin and currency orders and debiting of Customer's Account.

2. Money Room Cash and Check Deposits.

2.1 With respect to money room cash and check deposit processing services, Customer shall directly engage and execute an agreement between Customer and an armored carrier company ("Armored Carrier") that is on Bank's approved list of Armored Carriers. Customer will disclose to Bank its chosen Armored Carrier and provide Bank with a copy of Customer's agreement with the Armored Carrier (hereinafter the "Armored Carrier Agreement") upon Bank's request. Customer will arrange for the Armored Carrier to retrieve and transport all U.S. or Canadian (the latter being subject to Bank's pre-approval and acceptance in limited geographic areas only) coin and currency ("Cash Deposits") and checks ("Check Deposits") (collectively, the "Deposits") from certain of Customer's locations. Bank will designate a Bank money room processing location (each a "Cash Processing Center") to which Armored Carrier shall deliver Customer's Cash Deposits. Customer will inform Bank of any requested changes to these arrangements. Customer will prepare all Deposits in accordance with Bank's Deposit Preparation Guidelines to ensure accurate and timely credit. Bank will provide Customer with a copy of Bank's Deposit Preparation Guidelines.

2.2 At the time of pick-up of the Deposits, the Armored Carrier will sign-off on a log that is maintained at Customer's location(s) which indicates the date, time and bar code for each plastic bag associated with the Deposits. The Armored Carrier will transport the Deposits to Customer's Bank-designated Cash Processing Center in the same condition as they were received. The Cash Processing Center will count all Cash Deposits and record the total amount of funds to be credited on Bank's books and records

as a Cash Deposit to Customer's Account(s). To the extent the Deposits include Check Deposits, Bank shall arrange for transport of those Check Deposits to a Bank-designated Bank check processing location (each a "Check Processing Center").

2.3 In accordance with the Bank's Deposit Preparation Guidelines, Cash Deposits shall be prepared separately from Check Deposits and bundled separately by Customer for pick-up by Customer's Armored Carrier and delivery to Bank's Cash Processing Center.

2.4 Bank will provide Customer with same-Business-Day provisional credit for Cash Deposits received from the Armored Carrier by the Bank-designated Cash Processing Center in accordance with the Cash Processing Center's cut-off time of 6:00 pm. ET. Bank is not responsible if Customer's Armored Carrier does not deliver to the Bank-designated Cash Processing Center in time to meet the same-Business-Day provisional credit cut-off time. Credit may not be issued same-Business-Day if the Deposits are not prepared in accordance with Bank's Deposit Preparation Guidelines. Deposits remain the sole and exclusive property of Customer until Customer's Armored Carrier has delivered the Deposits to Bank's Cash Processing Center. Bank will not be responsible for any loss, theft, damage or destruction of the Deposits upon Customer's Armored Carrier pick-up of the Deposits until delivery to Bank's Cash Processing Center.

2.5 Customer acknowledges and agrees that it may only use the Services in connection with deposits to its own Account(s) with Bank. Customer agrees that no third parties, including employees of Customer, may use the Services for deposits to accounts other than Customer's Account(s). Without limiting the foregoing, should Customer permit any such third party usage, Customer agrees to defend, indemnify and hold Bank harmless from any claims by such third parties, including, but not limited to, those arising from the loss, damage or alteration of the third party deposit(s).

3. Currency Requisitions.

3.1 Customer may initiate a request for coin and currency (a "Cash Order") via a Bank-designated Cash

Processing Center's automated touchtone system, or, by special arrangement with Bank only, via Bank's local branch office(s). Cash Orders via Bank's automated touchtone system shall be initiated by Customer using its Bank-issued User ID and personal identification number ("PIN"). The ordering deadline for Cash Orders on a Business Day for delivery the following Business Day varies by Cash Processing Center. Cash Orders must be made by the designated Cash Processing Center's ordering deadline on a Business Day for the Armored Carrier's pick-up on the following Business Day.

3.2 For Cash Orders placed by Customer in accordance with this Section 3, Bank will fulfill Customer's Cash Order and debit Customer's Account on the Business Day prior to the Business Day for pick-up by Customer's Armored Carrier. Cash Orders on a Customer Account with insufficient funds may not be processed, in Bank's sole and exclusive discretion. Cash remains the sole and exclusive property of Bank until Customer's Armored Carrier signs the Bank-designated Cash Processing Center's manifest confirming Customer's Armored Carrier's pick-up of the Cash Order. Bank will not be responsible for any loss, theft, damage or destruction of the Cash Order upon Customer's Armored Carrier signing the Cash Processing Center's manifest confirming the Armored Carrier's pick-up of the Cash Order.

4. Armored Carrier as Customer's Authorized Agent and Independent Service Provider.

4.1 Customer represents and warrants that its Armored Carrier is acting as Customer's duly authorized agent at all times when interacting with Bank as described in this Appendix. Customer authorizes Bank to rely upon that authorization when interacting with Customer's Armored Carrier. Customer agrees that Bank's reliance on the foregoing when interacting with Customer's Armored Carrier shall be deemed reasonable, and further agrees to defend, indemnify, and hold Bank harmless from any and all claims, demands, damages, and liabilities (including reasonable attorneys' fees and expenses) directly or indirectly arising out of or incurred by reason of the Armored Carrier interacting with Bank as an agent for Customer.

4.2 Customer acknowledges and agrees that (i) Bank does not own or control the Armored Carrier; (ii) the Armored Carrier retains the discretion to determine what customers and geographic areas it will serve and maintains the ultimate responsibility for scheduling, movement and routing; (iii) the Armored Carrier acts as Customer's exclusive agent when Deposits are in transit and is responsible for the Deposits during transit; and (iv) the Armored Carrier is responsible for maintaining adequate insurance covering theft, employee fidelity and other in-transit losses. Bank is not and shall not be considered an insurer of any Deposits or other property placed with or under or in the possession, care, custody and/or control of the Armored Carrier. Deposits delivered by Customer to the Armored Carrier will be deemed deposited only when delivered to Bank and credited to Customer's Account as described in this Appendix.

5. Disputes Regarding Validity of Instructions; Deliveries.

5.1 Customer agrees that any and all disputes, claims, controversies, or causes of action that it may have now or in the future that are or may be directly or indirectly related to either (a) the legitimacy, accuracy, or timeliness of arrival of any Deposits to the Bank-designated Cash Processing Center, or (b) the pick-up of Cash Orders by Customer's Armored Carrier from the Bank-designated Cash Processing Center, shall be solely and exclusively between the Armored Carrier and Customer. Customer agrees that Bank shall be held harmless and excluded from any and all such matters.

5.2 Customer further agrees that Bank may make any and all adjustments to amounts deposited to or withdrawn from Customer's Account(s) if, subsequent to receipt and/or processing of a Deposit or a Cash Order, Bank discovers or becomes aware of a discrepancy, error in or omission from such Deposit or Cash Order. The parties understand and agree, however, that this right of correction and adjustment shall be at Bank's sole and exclusive discretion and shall not create any obligation or duty of Bank to examine, inspect, scrutinize or question any Deposit or Cash Order it receives from Customer or its Armored Carrier.

6. **Adjustments to Cash Order(s).** Customer will verify each Cash Order within twenty-four (24) hours of its receipt. In the event Customer believes there is a discrepancy with a delivery of a Cash Order, Customer must send a written notice of discrepancy to Bank no later than ten (10) Business Days after Customer's receipt of the Cash Order. The written notice shall be on Customer's letterhead, signed by an Authorized Signer on the Account, and shall describe the discrepancy and request research and resolution of the discrepancy. Customer should include originals of any currency straps involved, and copies of any and all Bank materials provided with the Cash Order delivery. If Customer fails to notify Bank within such time period, and Bank is required to adjust Customer's Account, Bank will not pay interest to Customer on the amount of the adjustment.

7. **Adjustments to Check Deposits and Cash Deposits.** Bank shall also have the right to make any and all adjustments to the amount to be credited to Customer's Account(s) as a Check Deposit or Cash Deposit if, subsequent to Bank's receipt and/or processing, Bank discovers or becomes aware of a discrepancy, error or omission in the Deposit.

8. **Availability of Deposits.** Customer understands and agrees that the availability for withdrawal, including for the fulfillment of any Cash Order(s), of any deposit of Cash Deposits or Check Deposits, shall be governed by the funds availability provisions of this Appendix and the Account Agreement, as the same may be amended from time to time.

9. **Additional Customer Warranties.** In addition to

the other warranties in this Appendix and the Cash Management Master Agreement, Customer represents and warrants that: (a) Customer will obtain the right from the Armored Carrier to provide a copy of the Armored Carrier Agreement to Bank; (b) Customer has given all necessary consents and approvals to the Armored Carrier allowing the Armored Carrier to provide Bank with the Deposits; (c) Customer and/or the Armored Carrier as Customer's agent shall safeguard the currency until it is physically delivered to Bank or Bank's agent; and (d) Customer will immediately notify Bank, and Customer will cause the Armored Carrier to immediately notify Bank, if there has been any breach of security related to the Armored Carrier activities hereunder or otherwise in conjunction with Customer's use of the Services.

10. Customer Request for Investigations. In addition to and not in lieu of Customer's obligations under this Appendix, the Cash Management Master Agreement or the Account Agreement, Customer may submit a written notice to Bank requesting an investigation of any loss, discrepancy or dispute relating to the performance and delivery of the Services. Customer agrees to provide such notice to Bank within thirty (30) Calendar Days of the event giving rise to the loss, discrepancy or dispute. Customer agrees to

cooperate fully, and cause its employees, agents, officers and contractors to cooperate fully, with Bank in any such investigation. If Customer fails to cooperate, or fails to provide notice to Bank within the time period required in this Section, Bank will be released from any obligation to investigate the loss, discrepancy or dispute, and will also be released from any liabilities, claims or expenses incurred by Customer or any third party in connection with such loss, discrepancy or dispute.

11. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable to or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the Services and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the Cash Management Master Agreement is terminated.



APPENDIX XXI

TD DATA TRANSMISSION SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and applies to TD Data Transmission Services made available to Customer by Bank or Bank's third-party service provider. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. **Services.** The Data Transmission Services (the "Services") provide Customer with the ability to exchange information files with Bank's (or its third-party service provider's) information systems for a variety of needs and functions. This Service allows Customer to send and/or receive its Bank files using File Transfer Protocol ("FTP"), Hypertext Transfer Protocol Secure ("Secure Web"), Secure File Transfer Protocol ("SFTP"), SWIFT Transmission, or via such other method as the parties may agree upon from time to time, as may be set forth in a Services' Setup Form(s), and as further described below.

2. **FTP Transmission.**

2.1 This method of data transmission permits Customer to deliver and/or receive encrypted files to a Bank-maintained FTP server. Bank will create a drop-box directory on the server where Customer may upload and deliver data files. To send data to Bank, Customer will either push the data files to Bank's directory, or Customer will give Bank a unique user name, password and Customer service address, and Bank will deliver the file. For data Bank sends Customer, Customer will pull the data files from its outbound directory on the server.

2.2 The technical requirements for FTP over the Internet include an Internet connection, FTP client capabilities, and Pretty Good Privacy ("PGP") or equivalent software for file encryption and decryption.

2.3 Files for transmission by FTP must be encrypted using PGP Version 4.0 or higher. PGP provides encryption technology including encryption, decryption, key management, encrypted email, digital signatures, key generation, certified keys and key revocation. Bank will generate a public key/private key pair for Customer. The public part of the key will be sent to Customer via Customer's assigned mailbox on Bank's transmission platform. The private part of the key will be securely kept within Bank. Customer will also generate a key pair for files that it sends to Bank. The public part of this key pair will be sent to Bank, also via the mailbox, while only Customer will know the private key.

2.4 To begin transmission by FTP, Bank will establish Customer's access to Bank's FTP server. Bank will provide Customer with the domain name required for the FTP connection. Customer will be provided a User ID and password that is unique to Customer and will be required each time Customer wishes to connect to Bank's transmission platform to send or receive files. PGP public keys for encryption will be exchanged. Bank and Customer will perform, to their mutual satisfaction, connectivity testing between platforms and encryption testing on transmitted files prior to Customer's use of the Service via FTP transmission.

3. **Secure Web Transmission.**

3.1 This method of data transmission permits Customer to deliver and/or receive files using an Internet connection, User ID and password. Bank will provide Customer with the domain name of a website that will display a web page with Customer's root directory. Customer can upload data files to this directory by clicking the Browse button and selecting the file from Customer's local network. Data files sent by Bank will be displayed in Customer's outbound directory and may be downloaded by Customer to its local network.

3.2 The technical requirements for Secure Web include an Internet connection and browser supporting 128-bit Secure Sockets Layer ("SSL") encryption.

3.3 Files for transmission through Secure Web are encrypted using SSL. SSL is an open protocol for securing data communication across computer networks that provides a secure channel for data transmission through its encryption capabilities. SSL allows for the transfer of digitally-signed certificates for authentication procedures and provides message integrity to protect against data being altered en route. Bank and Customer will perform, to their mutual satisfaction, connectivity testing between platforms and encryption testing on transmitted files prior to Customer's use of the Service via Secure Web.

4. Secure FTP (SFTP) Transmission.

4.1 This method of data transmission permits Customer to deliver to and/or receive files from a Bank-maintained SFTP server. Files transfers through SFTP communications are encrypted using Secure Shell ("SSH"). SSH is an open protocol for securing data communication across computer networks providing a secure channel for data transmission. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

4.2 Customer has the option to push files to Bank's SFTP server or have Bank pull Customer's files. For Customer push, Bank will create a drop-box directory on the SFTP server and provide Customer with a user name, password, and URL/domain name. Customer must provide an external IP address of the location sending files so that Customer's IP address can be added to access control lists within Bank's firewalls. For Bank to pull Customer's files, Bank will need a user name, password, URL/domain name, and directory from Customer so that Bank can pull files from Customer's SFTP servers. Bank and Customer will perform, to their mutual satisfaction, connectivity testing between platforms prior to Customer's use of the Services.

4.3 Customer also has the option for Bank to push Customer files (recommended by Bank) or Customer can pull the files from Bank's SFTP server. For Bank to push Customer's file, Bank needs Customer's URL/domain name, unique user name, password, and directory. For Customer to pull files from Bank's SFTP server, Customer must provide the external IP address of the location pulling the files so that Customer's IP address can be added to access control lists within Bank's firewalls. If Customer chooses to pull files from Bank's SFTP server, then files must be PGP encrypted, since files will reside on an SFTP server within Bank's DMZ. Bank will need Customer's public PGP key so that Bank can encrypt files. Bank and Customer will perform, to their mutual satisfaction, connectivity testing between platforms and encryption testing (if necessary) on transmitted files prior to Customer's use of the Services.

4.4 Customer will need an FTP client capable of using the SSH protocol. If Customer decides to pull files from Bank, Customer will need an application/utility capable of creating a PGP key pair and decrypting PGP files.

5. Secure Software.

5.1 This method of data transmission involves the use of a Java®-based program that serves as a secure access channel through which information may be exchanged between Customer's Computer and Bank. This software is provided by Bank and must be installed on a Customer's Computer or network. Secure Software facilitates the secure transfer of files both to and from Customer's network location.

5.2 The technical requirements for Secure Software include an Internet connection.

5.3 Files for transmission through Secure Software are encrypted using SSL. SSL is an open protocol for securing data communication across computer networks that provides a secure channel for data transmission through its encryption capabilities. SSL allows for the transfer of digitally-signed certificates for authentication procedures and provides message integrity to protect against data being altered en route. Bank and Customer will perform, to their mutual satisfaction, connectivity testing between platforms and encryption testing on transmitted files prior to Customer's use of the Services via Secure Software.

6. SWIFT Transmission.

6.1 This method of transmission provides Customer with the ability to use Society of Worldwide Interbank Financial Telecommunications operating as S.W.I.F.T. SCRL, Limited Liability Cooperative Society ("SWIFT") messaging services as described in this Section to engage in certain electronic communications with Bank (hereinafter the "SWIFT Services"). With the SWIFT Services, Customer may: (1) transmit certain SWIFT messages and documents to Bank and receive certain SWIFT messages and documents from Bank and other financial institutions, using SWIFT FIN and/or SWIFTNet FileAct, the latter of which is a file transfer service that allows the transmission of messages and documents over the SWIFT network in all formats agreed upon by Bank, and (2) transmit and receive SWIFT Instructions (as further described below) from Bank and other financial institutions in connection with certain Cash Management Services as agreed by the parties from time to time. Bank is a participating depository financial institution in SWIFT.

6.2 SWIFT Rules. The "SWIFT Rules" are the documents and other publications as amended by SWIFT from time to time that Customer may access at www.swift.com, whether in paper or electronic format, providing specific terms and conditions and other details relating to the provision and use of the SWIFT Services, including without limitation the SWIFT Contractual Arrangements; the SWIFT General Terms and Conditions; the SWIFT Service Bureau Policy and the SWIFT Data Retrieval Policy; the SWIFT MA-CUG, SCORE and TRCO Service Descriptions and any other SWIFT Service Descriptions applicable to the SWIFT Services; and the SWIFT On-line Support Service information. This Appendix, the SWIFT Services provided hereunder and the rights and obligations of the parties hereto shall be subject to the SWIFT Rules, as they may be amended from time to time. The parties agree to comply with the SWIFT Rules and to be aware of and comply with changes or updates to the SWIFT Rules.

6.3 SWIFT Instructions.

6.3.1 Bank may honor and act upon any authenticated SWIFT message, communication or instruction, including any Payment Order (hereinafter a "SWIFT Instruction") received in Customer's name or under

any SWIFT Business Identifier Code (BIC) that: (1) is unique to Customer, (2) is owned by a parent company or other affiliate of Customer, or (3) is owned by an unrelated third party and/or that is otherwise operating by agreement with Customer as Customer's agent for purposes of Customer's use of the SWIFT Services. Each such BIC(s) shall be identified by or through Customer in the Services' Setup Form(s) (hereinafter, collectively, "Customer's BIC(s)"). Customer acknowledges that the Services' Setup Form(s) shall also set out the key features and requirements that shall apply to Customer's use of the SWIFT Services, which may include but are not limited to the following:

- i. the SWIFT messaging services to be used to transmit SWIFT Instructions to Bank (e.g., SWIFT FIN and/or SWIFTNet FileAct);
- ii. the SWIFT message types and file formats that are supported by Bank under the SWIFT Services, including the types of Payment Orders that Customer may transmit;
- iii. the technical parameters associated with and required for SWIFTNet FileAct (e.g., file transfer mode options and file transfer fields, etc.);
- iv. the type of information that Bank shall provide in conjunction with any SWIFT message sent by Bank to Customer within the SWIFT Services, including any account status or other information made available by Bank;
- v. the Customer Account(s) to be used in connection with the SWIFT Services; and
- vi. the SWIFT access model (e.g., SCORE, MA-CUG, etc.) and connectivity (e.g., direct access, Alliance Lite, member, service bureau, etc.) associated with Customer's use of the SWIFT Services.

6.3.2 SWIFT Instructions made in accordance with this Appendix, the SWIFT Rules, and the Security Procedures (defined below) shall be deemed to have been given by an individual authorized to act on behalf of Customer. Bank will act in reliance on the accuracy and completeness of the SWIFT Instruction received by Bank in Customer's name or via Customer's BIC(s). Customer shall ensure that any SWIFT Instruction sent to Bank fully and accurately reflects the advice, request, instruction or communication intended to be provided to Bank by Customer and is duly authorized. Customer irrevocably authorizes Bank to (a) treat as accurate, authentic and properly authorized, rely upon and implement any SWIFT Instruction made in accordance with this Appendix, the SWIFT Rules, and the Security Procedures received by Bank which originates (or appears to originate) from Customer (including, in the case of a Payment Order, debiting the Account as specified in the SWIFT Instruction), and (b) to process each such SWIFT Instruction as described in this Section 6.

6.3.3 Notwithstanding the foregoing, Bank is not obligated to act on a SWIFT

Instruction or treat a SWIFT Instruction as accurate, authentic or authorized, if:

- the SWIFT Instruction does not meet the requirements of the SWIFT Rules or otherwise appears not to have been prepared or sent in accordance with this Section;
- Bank considers that the execution of that SWIFT Instruction may place Bank in breach of any law or regulation; or
- Bank reasonably suspects that the SWIFT Instruction received by Bank (a) may not fully and accurately reflect an advice, request, instruction or communication that Customer intended to give to Bank; or (b) may not have been given in accordance with Customer's authorization procedures.

Except to the extent prevented by applicable law or regulation, Bank shall notify Customer if, under this Section 6.3, it does not act on a SWIFT Instruction.

6.4 Secure Communications Channel.

6.4.1 SWIFT offers SWIFT messaging services as a secure communications channel. SWIFT has established procedures and requirements for controlling access to SWIFT messaging services (each, an "Access Control") that may include, without limitation, access codes, message authentication codes, secure card readers, digital signatures, and hardware security modules. In addition, SWIFT authenticates certain messages based on SWIFT message type prior to accepting them for routing as SWIFT Instructions (each, an "Authenticated Message"). This authentication may include confirming that the sender and recipient of the message have exchanged bilateral keys ("BKE"), entered into a relationship management application ("RMA") agreement, or taken other steps to secure the transmission of SWIFT Instructions between them as SWIFT requires from time to time (each, an "Authentication Procedure"). Collectively, the Access Controls and Authentication Procedures shall be referred to herein as the "SWIFT Security Procedures."

6.4.2 Bank and Customer rely on SWIFT's Access Controls and, in the case of an Authenticated Message, the Authentication Procedures, if any, that SWIFT requires to secure the transmission of Customer's SWIFT Instructions. Bank does not undertake and will have no obligation to Customer to separately authenticate any SWIFT Instruction that Bank receives in Customer's name or under Customer's BIC, whether or not Customer actually issued the SWIFT Instruction. Bank may, at Bank's sole election and option, contact Customer with respect to any SWIFT Instruction that Bank receives in Customer's name or under Customer's BIC, but Bank's election to contact Customer with respect to one or more SWIFT Instruction will not obligate Bank to contact Customer with respect to

subsequent SWIFT Instructions that Bank receives in Customer's name or under Customer's BIC.

6.5 Customer Representations and Warranties. Customer represents and warrants with respect to itself and the Customer's BIC(s) identified by or through Customer in the Services' Setup Form(s) that it:

- is registered with SWIFT as either a "Member Administered Closed User Group" and/or "Closed User Group" and/or "SCORE (Standardized Corporate Environment)" member;
- is in compliance with applicable SWIFT Rules;
- is not in violation of any applicable federal, state or local laws with respect to the SWIFT Services;
- is a duly organized and validly existing legal entity;
- is in good standing financially and in compliance with all laws and regulations applicable to Customer; and
- is subject to regular audits in accordance with internationally recognized accounting standards by independent auditors.

6.6 Third-Party Service Providers; Third Party-Service Provider Activities.

6.6.1 Customer may appoint a third party, whether a SWIFT registered user/member, SWIFT authorized service bureau or other third party, to send or receive SWIFT Instructions, perform other functions and/or otherwise act as Customer's agent for purposes of the SWIFT Services provided hereunder (a "Third-Party Service Provider"), as shall be set forth in the Services' Setup Form(s). In such event, Customer agrees that the Third-Party Service Provider shall have all the powers of Customer in relation to the SWIFT Services. Customer unconditionally authorizes Bank to deal directly with the Third-Party Service Provider in connection with all matters relating to the SWIFT Services, including, without limitation, the receiving and sending of SWIFT Instructions (including Payment Orders), and any testing to be completed with respect to the SWIFT Services. All SWIFT Instructions made in accordance with this Appendix, the SWIFT Rules, and the Security Procedures received by Bank from Third-Party Service Provider are hereby authorized by Customer. All acts and omissions of Third-Party Service Provider shall be the acts, omissions and responsibility of Customer and shall be governed by the provisions of this Appendix. For the avoidance of doubt, Customer shall ensure the Third-Party Service Provider complies with the relevant provisions of this Appendix. Notice of any termination of Third-Party Service Provider's authority to receive and send SWIFT Instructions to Bank on Customer's behalf shall be given to Bank in writing. The effective date of such termination shall be ten (10) Business Days after Bank receives written notice of such termination. Notwithstanding the foregoing, Customer agrees that Bank retains the right to reject any such Third-Party Service Provider and thus any associated

SWIFT Instructions initiated by Customer's Third-Party Service Provider in Bank's sole discretion.

6.6.2 Subject to Bank's prior approval and in its sole and exclusive discretion, Customer may be permitted to use the SWIFT Services provided hereunder on behalf of and in conjunction with Accounts that belong to Customer's clients, as well as on Customer's own behalf. Customer shall provide an appropriate letter of authority and/or execute any such other agreement(s) or documents as deemed necessary or appropriate by Bank prior to the initiation or continuation by Customer of the SWIFT Services in the capacity of a third-party service provider. Customer agrees that Bank retains the right to reject any request by Customer to engage in such activities as well as any SWIFT Instructions by Customer in such capacity, in Bank's sole discretion. In the event Bank approves Customer's use of the SWIFT Services as a third-party service provider, then the following shall also apply:

(a) Customer represents and warrants to Bank that each Customer client has given Customer authority to access and engage in SWIFT Instructions with respect to its Accounts through use of the SWIFT Services to the same extent as if Customer owned them, including in the capacity of a "third party service provider;"

(b) each reference to "Customer" herein will be deemed to be a collective reference to Customer and each Customer client whose Accounts are included in Bank's implementation of Customer's set-up for the SWIFT Services;

(c) all of the provisions set forth herein will apply to the Customer client's Account(s) as if Customer owned them;

(d) each person who is authorized to act on Customer's behalf with respect to the SWIFT Services is also authorized to act on Customer's behalf to the same extent with respect to the Accounts of each Customer client whose Accounts are included in Bank's implementation of Customer's set-up for the SWIFT Services; and

(e) Customer shall be liable for all monetary, confidentiality and other obligations to Bank hereunder as they relate to Customer's use of the SWIFT Services for itself as well as each such Customer client. Customer agrees to notify Bank immediately if Customer's authority with respect to Customer's client(s) is revoked or changed.

6.7 Customer Direction and Limitation of Liability.

6.7.1 In the event that the BIC(s) identified by or through Customer in the Services' Setup Form(s) are owned by a parent company or other affiliate of Customer, or are owned by an unrelated third party and/or such third party is otherwise operating by agreement with Customer as Customer's Third-Party Service Provider for

purposes of the SWIFT Services, Bank is prepared to act on a SWIFT Instruction from Customer's SWIFT BIC(s) only upon receipt of the limitation of liability provided in this Section 6. This indemnity shall be in addition to and not in lieu of an additional limitation of liability provided by Customer in the Cash Management Master Agreement.

6.7.2 Bank is authorized to accept and honor any files and/or SWIFT Instructions sent from any of Customer's SWIFT BIC(s) without making any inquiry as to the validity or sufficiency of the SWIFT Instructions and to consider the SWIFT Instructions of like force and effect as written orders made in accordance with the signing authorities held by Bank from time to time for the operation of Customer's Account(s) with Bank.

6.7.3 Without limiting the scope of Section 6.7.2, Bank is authorized to disclose information about Customer, its Accounts and banking relationship with Bank, including any changes to such information, in response to and as directed in the SWIFT Instructions as required to process the same.

6.7.4 Bank shall not be liable for any loss or damage incurred by Customer, or any third party arising from or in any way related to Bank acting upon or refusing to act upon any SWIFT Instructions made in accordance with this Appendix, SWIFT Rules, and the Security Procedures from Customer's BIC(s), unless due to the gross negligence or willful misconduct of Bank. Notwithstanding the foregoing, in no event shall Bank be liable for any indirect, special or inconsequential damages incurred by Customer or any third party arising from or in any way related to Bank acting upon or refusing to act upon any SWIFT Instructions.

6.7.5 Customer agrees that Bank shall not be responsible or liable under this Agreement for any losses, liabilities, claims, damages, fees, or expenses whatsoever that are pursuant to, in connection with, or in any way related to Bank acting upon, delaying in acting upon or refusing to act upon any SWIFT Instructions from Customer's BIC(s).

6.8 Termination of SWIFT Services. In addition to but not in lieu of the provisions of the Cash Management Master Agreement, the SWIFT Services shall terminate automatically in the event that:

- either party loses user status as defined in the SWIFT General Terms and Conditions of the By-laws;
- SWIFT has ceased to provide, and not resumed providing, any of the SWIFT messaging services;
- SWIFT, in exercise of its rights under the SWIFT Rules, has required either party to terminate the SWIFT Services; or
- Bank has ceased to provide the Cash Management Services.

6.9 Suspension of SWIFT Services. In addition to but not in lieu of the provisions of the Cash Management Master Agreement, either party may suspend the use of the SWIFT Services for such period(s) as it considers appropriate in its absolute discretion by written notice to the other party if: (a) suspension is necessary for the purpose of (routine or emergency) maintenance; (b) for security or SWIFT Services for such period(s) as it considers appropriate in its absolute discretion by written notice to the other party if: (a) suspension is necessary for the purposes of (routine or emergency) maintenance; (b) for security or technical reasons, including a suspension of the SWIFT messaging services by SWIFT, use of the SWIFT messaging services is impossible or cannot be achieved without unreasonable cost to Bank or Customer; (c) suspension is required by SWIFT or the SWIFT Rules; or (d) suspension is necessary to avoid or reduce any material damage or disadvantage to either party.

7. Security Procedures.

7.1 Customer agrees that the security procedures set forth or incorporated by reference in this Appendix (including without limitation the SWIFT Security Procedures), the Cash Management Master Agreement and/or associated documents provided by Bank, including without limitation the Services' Setup Form(s), are a commercially reasonable method of providing security against unauthorized access to or interception of transmissions between Customer and Bank (hereinafter collectively the "Security Procedures"). Any transmission by Customer shall be deemed authorized if transmitted in accordance with the Security Procedures. Bank may, from time to time, modify the Security Procedures. Such modifications shall become effective upon receipt of notice by Customer or such later date as may be stated in the Bank's notice to Customer. If Customer fails to object to such change, it shall be deemed to agree to such change.

7.2 With respect to SWIFT in particular, Customer further acknowledges that the SWIFT Security Procedures are the only security procedures offered for SWIFT Instructions that Customer transmits through the SWIFT Services. Customer has solely determined that the SWIFT Security Procedures best meet Customer's requirements with regard to the size, type and frequency of the SWIFT Instructions issued by Customer to Bank using the SWIFT Services and that the SWIFT Security Procedures are a commercially reasonable method of providing security against unauthorized access to or interception of transmissions between Customer and Bank. Customer acknowledges that it is bound by the terms and conditions of each SWIFT Instruction, including any request to cancel or amend a SWIFT Instruction, whether or not authorized by Customer, that Bank receives in Customer's name or under Customer's BIC(s) through the SWIFT Services and in accordance with the SWIFT Security Procedures.

7.3 Nothing in this Appendix shall be deemed a representation or warranty by Bank that FTP, Secure Web, SFTP or SWIFT communications are secure. Rather, after

review of the alternatives, Customer has selected a communication method that it believes best suits its needs.

7.4 Bank and/or SWIFT (as applicable) may, from time to time, propose different, additional or enhanced security procedures to Customer. Customer understands and agrees that if it declines to use any such enhanced procedures, it will be liable for any losses that would have been prevented by such procedures. Notwithstanding anything else contained in this Appendix, if Bank and/or SWIFT believes immediate action is required for the security of Bank, SWIFT or Customer funds or data, Bank and/or SWIFT may initiate additional security procedures immediately and provide prompt subsequent notice thereof to Customer.

7.5 Customer hereby acknowledges that the Security Procedures are neither designed nor intended to detect errors in the content or verify the contents of a transmission between the parties. Accordingly, any errors contained in a transmission from Customer shall be Customer's responsibility. Except as otherwise expressly provided in the parties' Cash Management Master Agreement or other Appendix between the parties, no security procedure for the detection of any such Customer error has been agreed upon between Bank and Customer.

7.6 Customer is strictly responsible for establishing and maintaining procedures to safeguard against, detect and mitigate unauthorized access to or interception of transmissions. Customer covenants that no employee or other individual under Customer's control will be allowed to initiate transmissions in the absence of proper authority,

supervision and safeguards, and agrees to take reasonable steps to maintain the confidentiality of the Security Procedures and any passwords, codes, security devices and related instructions provided by Bank in connection with any Security Procedure utilized by Bank, SWIFT and/or Customer. If Customer believes or suspects that any such password, code, security device, Security Procedure, information or instructions have been disclosed to or accessed by unauthorized persons, Customer agrees to notify Bank immediately followed by written confirmation as provided in the Services' Setup Form(s).

7.7 Customer shall retain data files for five (5) Business Days following the date of their transmittal by Customer as provided herein, and shall provide such data files to Bank upon written request.

8. Effectiveness. Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to Data Transmission Services and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank and Customer or the parties' Cash Management Master Agreement is terminated.



APPENDIX XXII

TD ACH POSITIVE PAY SERVICES

This Appendix is incorporated by reference into the parties' Cash Management Master Agreement and applies to all TD Automated Clearing House ("ACH") Positive Pay Services (the "Services") made available to Customer by Bank. All capitalized terms used herein without definition shall have the meanings given to them in the Cash Management Master Agreement or the *NACHA Rules* (as defined below). Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Cash Management Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict.

TERMS AND CONDITIONS

1. Definitions.

"*Authorized Account*" means Customer's Account(s) designated by Customer and maintained at Bank to which the Services will apply.

"*ACH Entry*" means an order or request for the transfer of money to an Authorized Account (a "Debit Entry") as also defined in the *NACHA Rules*.

"*ACH Authorizations*" means Customer's written instructions and authorization criteria provided to Bank in conjunction with the set-up and implementation of the Services, including the Services' Setup Form(s) and/or via a separate ACH block and filter agreement with Bank (hereinafter the "Filter Agreement"), and/or otherwise in accordance with the Services as described in this Appendix, which either prohibits all ACH Entries or permits only the posting of specified ACH Entries to an Authorized Account.

"*Exception Entry*" means an ACH Entry (excluding ARC, BOC, POP, RCK, or XCK SEC Codes) that does not meet Customer's ACH Authorizations previously provided to Bank (and may also be referred to within the Services as a "Rejected" Entry), and that is therefore scheduled to be returned to the Originator of the ACH Entry.

"*NACHA Rules*" means the National Automated Clearing House Association's ("NACHA") *Operating Rules and Operating Guidelines*, which govern the ACH system.

"*Pay Decision(s)*" means Customer's confirmation instruction to Bank to pay/post an Exception Entry.

"*Return Decision(s)*" means Customer's confirmation instruction to Bank to not pay/post an Exception Entry but to instead return the ACH Entry to the Originator.

"*Return Default Disposition*" means the Services' automatic default disposition of all ACH Entries that do not meet Customer's ACH Authorizations, whereby all such ACH Entries are scheduled to be returned to the Originator of the ACH Entry.

2. Services.

2.1 The Services described in this Appendix will provide Customer with a means to: (1) review ACH Entries received on a particular Customer Account that are scheduled to be returned to the Originator as an Exception Entry in accordance with Customer's ACH Authorizations and the Return Default Disposition; and (2) confirm the return of the Exception Entry through a Return Decision, or to override the Return Default Disposition and instruct Bank to pay/post the Exception Entry to Customer's Account through a Pay Decision.

2.2 Customer acknowledges that the Services have been identified by Bank as a service that can reduce the risk of fraudulent ACH Entries being posted against Customer's Account(s) when such Services are adopted and properly utilized by Customer. By conforming to the terms and conditions of this Appendix, Customer acknowledges and agrees that it may significantly reduce the chance that fraudulent ACH Entries will post to Customer's Account(s) by electronically matching incoming ACH transactions to ACH Authorizations.

3. Customer Authorizations.

3.1 Customer will designate Authorized Account(s) to be used with the Services via the Services' Setup Form(s).

3.2 As applicable, Customer shall begin use of the Services with either: (a) any ACH Authorizations initially submitted by Customer to Bank and then established by Bank on Customer's behalf in conjunction with the set-up and implementation of the Services, or (b) any existing ACH Authorizations on Customer's Authorized Account(s) that have been established via a Filter Agreement. Customer may add to or modify those initial or existing ACH Authorizations from time to time as set forth herein. Customer shall be responsible for the accuracy and completeness of all information provided to Bank both through the use of the Services and via the Services' Setup Form(s).

3.3 Customer may submit additional ACH Authorizations, make changes to initial or existing ACH Authorizations, or delete initial or existing ACH

Authorizations related to the Authorized Account(s) online via the Services' module of the Bank Internet System. Such changes shall become effective on the next Business Day following the day on which the changes were made by Customer. Each Business Day, Bank will provide an updated list of successfully processed ACH Authorizations to Customer via the Services. In the event Customer submits a change or addition to the ACH Authorizations that is incomplete, contains an error or that cannot otherwise be processed by Bank, Bank will use commercially reasonable efforts to notify Customer on the next Business Day that the associated ACH Authorization(s) has been rejected. Until such time as Customer reviews and corrects it, the rejected ACH Authorization(s) will not appear on the updated list of successfully processed ACH Authorizations that Customer receives.

3.4 In the event Customer fails to fully and accurately populate or complete all requested fields associated with the ACH Authorizations, the following will also apply:

(a) If Customer does not insert a specified maximum dollar amount, then no maximum dollar amount shall apply with respect to the applicable ACH Entry(ies) or transaction(s) subject to the ACH Authorization(s).

(b) If Customer does not insert a specified expiration date, then no expiration date shall apply to the applicable ACH Entry(ies) or transaction(s) subject to the ACH Authorization(s).

4. Processing of ACH Entries and Reporting of Exception Entries. Bank will electronically compare each ACH Entry presented to Bank for settlement against Customer's Authorized Account(s) on a Business Day (including those presented by other depository institutions, ACH Operators or by Bank) with Customer's ACH Authorizations. In accordance with that review, on each Business Day, Bank will:

(a) allow incoming ACH Entries that match Customer's ACH Authorizations to post to Customer's Authorized Account(s); and

(b) treat as Exception Entries all incoming ACH Entries that do not match Customer's ACH Authorizations and will provide to Customer, through the Bank Internet System, a listing of all Exception Entries that are otherwise scheduled for Return Default Disposition. Customer must monitor, review and issue a Pay Decision or Return Decision on each Exception Entry reported through the Bank Internet System by the pre-established deadline set forth within the Services. Customer may also set up alerts to be sent to Customer by a pre-established time each Business Day advising Customer whether or not there are any Exception Entries to be reviewed that Business Day.

5. Payment and Dishonor of Exception Entries.

5.1 Customer may choose to confirm the Return Default Disposition of individual Exception Entries presented via the Services by providing a Return Decision to Bank by the pre-established deadline set forth within the

Services, in which case such Exception Entries will be automatically returned to the Originator.

5.2 Customer may choose to override the Return Default Disposition of individual Exception Entries presented via the Services by providing a Pay Decision to Bank by the pre-established deadline set forth within the Services, in which case such Exception Entries will be paid/posted to Customer's Authorized Account(s) at the end of the current Business Day.

5.3 Customer may choose not to or may otherwise fail to review and provide a Pay Decision or a Return Decision for any Exception Entries by the pre-established deadline, in which case the Return Default Disposition will apply and all such Exception Entries will be automatically returned to the Originator.

6. Customer and Bank Communications.

6.1 Customer shall use the Services' module of the Bank Internet System to report all Pay Decisions or Return Decisions. Bank shall not be obligated to comply with any Pay Decision or Return Decision received in a format or medium, after a pre-established deadline, or at a place not permitted under this Appendix or the Services' Setup Form(s), and may instead treat any such communication from Customer as a Return Decision or otherwise apply the Return Default Disposition to such communication.

6.2 Bank is not responsible for detecting any Customer error contained in any ACH Entries presented, decisioned, returned or processed, or in any Pay Decision or Return Decision by Customer.

6.3 In the event that Bank is unable to provide Customer with a listing of Exception Entries through the Bank Internet System for Customer's Pay Decision or Return Decision as described in Section 4, the Return Default Disposition shall apply in accordance with Customer's previously established ACH Authorizations.

6.4 Customer's ACH Authorizations hereunder will be accepted by Bank subject to the condition that ACH transactions have not already been posted or are not otherwise in the process of posting, and that Bank will have a reasonable opportunity to act on Customer's ACH Authorizations before any such processing.

6.5 Bank shall have a reasonable time after receipt of Customer's request to implement the Services and shall not assume responsibility for stopping ACH transactions that have already been posted to Customer's Account(s).

6.6 Bank shall be bound only to exercise ordinary care in attempting to post or return ACH Entries as described in this Appendix.

7. Remedies.

7.1 **Bank Liability.** To the extent permitted by applicable law, the liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the parties' Cash Management Master

Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer.

7.2 Wrongful Payment/Posting. It shall constitute wrongful payment/posting by Bank if Bank pays/posts an Exception Entry for which Customer has provided a Return Decision by the pre-established deadline set forth within the Services and otherwise in accordance with the other terms of this Appendix. In the event that there is wrongful payment/posting, Bank shall be liable to Customer for the lesser of the amount of the wrongfully paid/posted Exception Entry or Customer's actual damages resulting from Bank's posting of the Exception Entry, subject to the terms of the parties' Cash Management Master Agreement.

7.3 Rightful Payment and Return.

7.3.1 If Bank honors an Exception Entry in accordance with a Pay Decision by Customer as described in Section 5.2, such payment/posting shall be rightful, and Customer waives any right it may have to assert otherwise.

7.3.2 If Bank returns an Exception Entry in accordance with a Return Decision by Customer as described in Section 5.1, or otherwise pursuant to a Return Default Disposition as described in this Appendix, the return shall be rightful, and Customer waives any right it may have to assert otherwise.

7.3.3 Customer agrees that Bank exercises ordinary care whenever it rightfully pays/posts or returns an Exception Entry consistent with the provisions of this Appendix.

8. Other Terms of the Services.

8.1 Customer acknowledges that the Services do not preclude Bank's standard ACH processing procedures or the application of the *NACHA Rules*, which may cause an ACH Entry to be dishonored even if Customer's instructions do not otherwise require Bank to return such ACH Entry.

8.2 Customer acknowledges that the Services do not apply to transactions between Customer and Bank, including any Bank affiliates and subsidiaries, such as loan or credit card payments ("Bank-Related Entries"). Bank is permitted to pay Bank-Related Entries whether or

not Customer has included these in Customer's ACH Authorizations as reflected in this Appendix and until such time as Customer's authorization with respect to the underlying Bank-Related Entries is revoked or otherwise terminated.

8.3 Customer acknowledges that the Services are intended to be used to identify and return ACH Entries which Customer suspects in good faith are fraudulent, unauthorized or otherwise unwarranted. The Services are NOT intended to be a substitute for authorization instructions or to delay Customer's decision on ACH Entries, including but not limited to stop payment orders on ACH Entries which are not suspected in good faith to be unauthorized. If Bank suspects or deems, in Bank's sole discretion, that Customer is using the Services contrary to those intentions, Bank may require Customer to provide evidence that ACH Entries that Bank returns pursuant to Customer's instructions were in good faith suspected to be unauthorized. In addition, Bank may hold Customer liable for actual losses that Bank sustains on ACH Entries which Bank is requested to return under the Services and which Customer does not reasonably establish as unauthorized ACH Entries, as provided under the *NACHA Rules*.

9. Termination; Effectiveness.

9.1 The parties may terminate this Appendix and/or the Services in accordance with the terms and conditions of the Cash Management Master Agreement. This Appendix and the associated Services shall automatically terminate in the event the underlying Authorized Account(s) are closed. In the event of termination of this Appendix and the associated Services, Customer's ACH Authorizations in effect as of the date of termination will remain in effect with respect to Customer's Authorized Accounts, and all ACH Entries will thereafter be processed in accordance with such ACH Authorizations.

9.2 Each of Bank and Customer agrees to all the terms and conditions of this Appendix. The liability of each of Bank and Customer under this Appendix shall in all cases be subject to the provisions of the Cash Management Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank or Customer. This Appendix replaces and supersedes all prior agreements on file with respect to the Services, except for any existing ACH Authorizations currently on record with regard to the Authorized Account(s) as of the date of this Appendix.

Remainder of page intentionally left blank.

TECH VALLEY REGIONAL TECHNOLOGY INSTITUTE

STATEMENT OF NET POSITION

JUNE 30, 2021

Assets and Deferred Outflows of Resources**Current Assets:**

Cash	\$ 1,332,493
State and Federal Aid Receivable	179,549
Total Current Assets	<u>1,512,042</u>

Noncurrent Assets:

Capital Assets - Net	<u>386,702</u>
Total Assets	<u>1,898,744</u>

Deferred Outflows of Resources:

Pension	791,617
OPEB	<u>291,222</u>
Total Deferred Outflows of Resources	<u>1,082,839</u>

Total Assets and Deferred Outflows of Resources	<u>\$ 2,981,583</u>
---	---------------------

Liabilities and Deferred Inflows of Resources**Current Liabilities:**

Accounts Payable and Accrued Expenses	\$ 23,912
Due to Retirement Systems	<u>149,038</u>
Total Current Liabilities	<u>172,950</u>

Noncurrent Liabilities:

Proportionate Share of Net Pension Liability	213,268
Accrued Other Postemployment Benefits	<u>2,414,507</u>
Total Noncurrent Liabilities	<u>2,627,775</u>

Total Liabilities	<u>2,800,725</u>
-------------------	------------------

Deferred Inflows of Resources

Pension	267,634
OPEB	<u>1,275,701</u>
Total Deferred Inflows of Resources	<u>1,543,335</u>

Net Position (Deficit)

Invested in Capital Assets	386,702
Unrestricted (Deficit)	<u>(1,749,179)</u>
Total Net Position (Deficit)	<u>(1,362,477)</u>

Total Liabilities, Deferred Inflows of Resources and Net Position (Deficit)	<u>\$ 2,981,583</u>
--	---------------------

TECH VALLEY REGIONAL TECHNOLOGY INSTITUTE

NOTES TO FINANCIAL STATEMENTS (CONTINUED)

JUNE 30, 2021

6. PENSION PLANS (CONTINUED)

Discount Rate

The discount rate used to calculate the total pension liability was 7.10% for TRS and 5.9% for ERS. The projection of cash flows used to determine the discount rate assumes that contributions from plan members will be made at the current contribution rates and that contributions from employers will be made at statutorily required rates, actuarially determined. Based upon the assumptions, the System's fiduciary net position was projected to be available to make all projected future benefit payments of current plan members. Therefore the long term expected rate of return on pension plan investments was applied to all periods of projected benefit payments to determine the total pension asset or liability.

Sensitivity of the Proportionate Share of the Net Pension Asset/Liability to the Discount Rate Assumption

The following presents the Institute's proportionate share of the net pension (asset)/liability calculated using the discount rate of 7.10% (TRS) and 5.9% (ERS), as well as what the Institute's proportionate share of the net pension (asset)/liability would be if it were calculated using a discount rate that is 1-percentage point lower or 1-percentage point higher than the current rate:

	<u>1% Decrease</u>	<u>Current Assumption</u>	<u>1% Increase</u>
<u>TRS</u>			
Employer's proportionate share of the net pension liability	\$ 1,345,078	\$ 212,942	\$ (737,208)
<u>ERS</u>			
Employer's proportionate share of the net pension liability	\$ 93,278	\$ 336	\$ (85,378)

Pension Plan Fiduciary Net Position

The components of the net pension liability (TRS and ERS) of the employer as of June 30, 2020 and March 31, 2021, respectively, were as follows (in thousands):

	<u>TRS</u>	<u>ERS</u>
Employers' total pension liability	\$ (123,242,776)	\$ (220,680,157)
Plan fiduciary net position	120,479,505	220,580,583
Employers' net pension liability	\$ (2,763,271)	\$ (99,574)
Ratio of plan fiduciary net position to the employers' total pension liability	<u>97.80%</u>	<u>99.95%</u>

TECH VALLEY REGIONAL TECHNOLOGY INSTITUTE

NOTES TO FINANCIAL STATEMENTS (CONTINUED)

JUNE 30, 2021

7. OTHER POSTEMPLOYMENT BENEFITS (CONTINUED)**Total OPEB Liability**

The Institute's total OPEB liability of \$2,414,507 was measured as of June 30, 2021 and was determined by an actuarial valuation as of July 1, 2020.

Actuarial Assumptions and Other Inputs - The total OPEB liability in the July 1, 2020 actuarial valuation was determined using the following actuarial assumptions and other inputs, applied to all periods included in the measurement, unless otherwise specified:

Accrual Cost Method	Entry age normal
Salary Increases	2.6 percent, average, including inflation
Discount Rate	2.16 percent
Healthcare Cost Trend Rates	5.3 to 4.1 percent over 55 years
Retirees' Share of Benefit-Related Costs	100 percent of projected health insurance premiums for retirees

The discount rate was based on the Bond Buyer General Obligation 20 Year Municipal Bond Index.

The valuation reflects the adoption of the Pub-2010 Mortality Table (from RP-2014 adjusted to 2006 Total Dataset Table) with generational projection of future improvements per the MP-2019 Ultimate Scale.

Covered Payroll	<u>\$ 1,160,883</u>
-----------------	---------------------

Changes in the Total OPEB Liability

Balance at June 30, 2020	<u>\$ 159,970</u>
<u>Changes for the Year -</u>	
Service cost	18,652
Interest on total OPEB liability	3,947
Effect of plan changes *	2,040,275
Effect of demographic gains or losses	(90,307)
Effect of assumptions changes or inputs	<u>281,970</u>
Net Changes	<u>2,254,537</u>
Balance at June 30, 2021	<u>\$ 2,414,507</u>

* Effect of plan changes of \$2,040,275 is primarily a result of teachers now being eligible for postemployment benefits.

Tech Valley High School

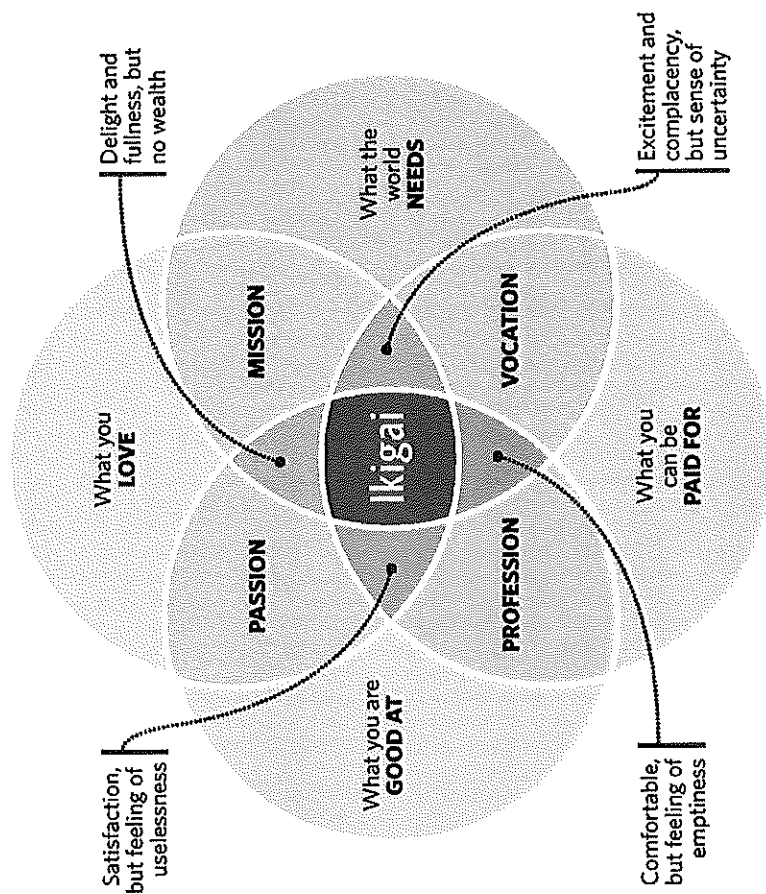
Principal's Report
Operating Board
January 27, 2022

Tech Valley High School provides a unique and innovative student-centered educational opportunity, engages students in current emerging technologies, and supports the growth and economy of the region.



Ikigai

A JAPANESE CONCEPT MEANING "A REASON FOR BEING"



SOURCE: dreamstime

TORONTO STAR GRAPHIC

TechValley
HIGH SCHOOL

I-Term 2022

Freshman:

Any topic - Poster Presentation,
Reflection

Sophomore:

Extreme Exposure/Careers
Exploration, Reflection and Pecha Kucha

Juniors:

Research Paper, DIY, Ted Talk, Reflection,
Digital Portfolio

Seniors:

Happiness Project: Research Paper, 2 week experience with business partners, Interview, Evidence of Learning, Digital Portfolio, 360 ° perspective of topic (careers)

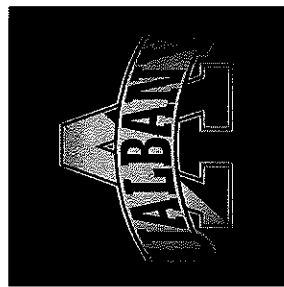
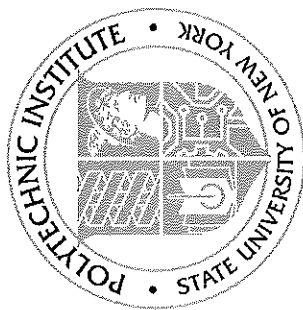
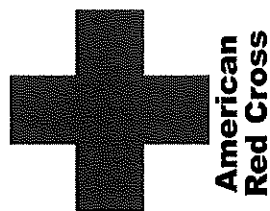


I-Term 2022

I-Term Rollout

- Navigating Your Career Path by Miriam Dushane, Alaant Workforce Solutions
- Alumni Day
- Introduction to Data Literacy - inspired by Business Alliance
- Interview Skills

I-Term 2022



**ADIRONDACK
STUDIOS**

**HINMAN
STRAUB**
ATTORNEYS AT LAW



TRELLEBORG



a the REP ★

troywebconsulting

wmht

