

Queenstown Bank of Maryland
Business Online Banking Terms and Conditions

These are the terms of your Agreement with Queenstown Bank for accessing your accounts and making use of other services via the Internet through Queenstown Bank. Whenever you use Internet Banking, or authorize others to use it, you agree to these terms. Queenstown Bank may amend these terms from time to time. You will be notified of any amendments that affect your rights or obligations within the appropriate time period. Each of your accounts at Queenstown Bank, which are accessed by Internet Banking continue to be governed by the applicable Account Disclosures and Regulations Relating to Deposit Accounts and Other Services and Electronic Fund Transfer Agreement and Disclosures, otherwise known as Disclosures and Regulations, and the applicable Schedule of Fees, as they may be amended from time to time.

GENERAL INFORMATION

1. Definition of Terms

- "You", "User" and "Your" means any person who applies for Internet Banking with Queenstown Bank through completion of the Queenstown Bank Internet Banking Application and all persons authorized by the applicant to use their Internet Banking Identification and PIN (Personal ID Number) or other means of access we establish or approve.
- "We," "Us," "Our," "Bank," "Financial Institution," and "Queenstown Bank" refer to the Queenstown Bank of Maryland.
- "Business Day" shall mean Monday-Friday, except for federal banking holidays.
- "Online Banking Agreement" or "Agreement" means the Queenstown Bank Business Online Banking Terms and Conditions.
- "Internet Banking" or "The Service" or "Business Online Banking" means our service that allows you to make payments, transfer funds, access accounts, make purchases, obtain information, and perform other transactions via the Internet by use of a personal computer and modem and/or other means we authorize or allow.
- "Security Codes," refers to any combination of a "Users" Access ID and Password

2. General Description of Available Services

Account access via Queenstown Bank's Internet Banking Service allows you to:

- View account balances and transaction history for up to 90 days on accounts
- Transfer funds between Queenstown Bank accounts
- Set up recurring transfers between Queenstown Bank accounts
- Make loan payments on your Queenstown Bank loan accounts
- Download account transactions to your third-party accounting software
- Add or review stop payments orders on accounts
- Initiate bill payments upon enrollment of Bill Pay Services.
- View images of paid checks and processed deposit transactions on accounts
- Administrative features include adding, modifying, and deleting users for online banking access

3. Requirements for Your Use

To access your accounts through Business Online Banking, you must have a Queenstown Bank account and complete the Business Online Banking Enrollment process. In addition, you will need a personal computer and an Internet browser that supports 128-bit data encryption and Transport Layer Security (TLS) v1.2. You will need Internet access through the service provider of your choice (ISP). Business Online Banking is viewed best with Microsoft Internet Explorer versions 11 or higher. Other browsers may work, but the display and printing of pages may not be ideal. You need access to a printer and/or other storage medium, such as a hard drive for downloading information or printing disclosures. An external email address is required for the delivery of electronic statements, notices, and disclosures. To view images within Business Online Banking you will need to have the latest versions of both Adobe Flash Player and Adobe Acrobat Reader installed. Prior to enrolling in the service you should verify that you have the required hardware and software necessary to access Business Online Banking and retain a copy of these terms and conditions. If we revise hardware and software requirements that may impact your ability to

access Business Online Banking, we will give you advanced notice of these changes and give you an opportunity to cancel and/or change your method of receiving electronic disclosures (e.g. change to paper format vs. electronic format) without the imposition of any fees.

You are responsible for the installation, maintenance and operation of your computer and your browser software. The risk of error, failure, or non-performance is your risk and includes the risk that you do not operate your computer or your software properly. The Bank is not responsible for any errors or failures from any malfunction of your computer or your software. Queenstown Bank is not responsible for any electronic viruses that you may encounter. The Bank is not responsible for any computer virus-related problems that may be associated with the use of Business Online Banking. The Bank has no liability to you for any damage or other loss, direct or consequential, which you may suffer or incur by reason of your use of your computer or your software.

4. Enrollment Process

Business customers interested in the commercial features of the Service should visit one of our eight conveniently located branches and speak to a Branch Manager or contact our Operations Department directly at (410) 827-8881. Queenstown Bank will provide you with an application for Business Online Banking, titled “Business Online Authorization Worksheets.” Upon receipt of the application our Operations Department will verify the information provided for accuracy and proper authorizations.

5. Password Requirements

When your Business Online Authorization Worksheets have been received, and the review is completed, we will assign you an Access ID and temporary password, which you will use for your first login. You will then be prompted to build a new password for your Access ID, which must be a minimum of 8 characters, no more than 17 in length, and include at least 2 numbers and 1 special character. You will also be prompted to answer 3 security challenge questions/answers that will assist with authenticating your identity. Your Access ID cannot be modified once established and you will be prompted every 365 days to change your password. Password requirements may differ for users approved to originate ACH transactions and/or use Remote Deposit Capture. Please refer to the applicable section in these terms and conditions for more information.

6. Password Responsibilities

When you accept the terms and conditions of this Agreement, you agree not to give or make available your password or other means to access your account to any unauthorized individuals. You are responsible for all transfers and Bill Payments you authorize using Business Online Banking. If you or your Authorized users disclose your Password to anyone, and/or if you allow someone to use your Password to access your accounts, you are authorizing them to act on your behalf and you will be responsible for any use of the Service by them (e.g., such as when you provide this information to a joint account holder, an employee, and/or an aggregation service provider).

If you believe that your password or other means to access your account has been lost or stolen or that someone may attempt to use the Service without your consent or has transferred money without your permission, you must notify us at once by calling (410) 827-8881 during customer service hours. We also recommend that you immediately log into the system and change your Business Online Banking password.

In addition to the security features described above, there may be other security related notices posted on our website or Business Online Banking from time-to-time. It is your responsibility to read all security notices.

7. Linked Accounts

We will link the approved business accounts that were provided to us in writing during the Business Online application process. Additional accounts may be requested in writing.

8. Signature Requirements

When any transfer or other payment instruction is initiated through the Service for your benefit, you agree that we may debit the designated accounts without requiring your signature on the item and without any notice to you. Accounts that have entered into a ‘two signatures required’ arrangement with Queenstown Bank of Maryland are prohibited in Business Online Banking.

9. Account Balances

Balances shown in your accounts may include deposits subject to verification by us. The balance reflected may differ from your records due to deposits in progress, checks outstanding, or other withdrawals, payments or charges. A transfer request may not result in immediate availability because of the time required to process the request. A transfer request must be made before the Business Day cut-off time to be effective the same Business Day.

The balances are updated in real-time and will display the available balance. There may be situations that cause a delay in an update of your balances. Business Online Banking will use the memo available balance at the time of a transaction to base our approval for account transfers.

10. Hours of Accessibility

You can access your accounts through Business Online Banking seven days a week, 24 hours a day unless otherwise defined on the application. However, at certain times, Business Online Banking may not be available due to routine system maintenance.

11. Fees, Changes to Fees, or Other Terms

There are no monthly or transaction fees for accessing your account(s) through Business Online Banking. Bill pay services provided by CheckFree may be subject to a \$5.00 fee per statement cycle.

Queenstown Bank reserves the right to change the charges, fees or other terms described in the Business Online Banking Terms and Conditions. When changes are made to any fees, charges, or other material terms, we will update this Agreement and notify you accordingly. Notification will be given at least thirty (30) days in advance of the effective date of any additional fees for online transactions, or of any stricter limits on the type, amount or frequency of transactions or any increase in your responsibility for unauthorized transactions, unless an immediate change is necessary to maintain the security of the system. If such a change is made, and it can be disclosed without jeopardizing the security of the system, we will provide notice to you within thirty (30) days after the change. We reserve the option, in our business judgment, to waive, reduce or reverse charges or fees in individual situations. Changes to fees applicable to specific accounts are governed by the applicable Depositor Terms and Conditions and the deposit account information.

If approved to originate ACH transactions or make Remote Deposit Capture deposits, please see the ACH Origination or Remote Deposit Capture section in this document, for any applicable fees.

12. Transfers

Through Business Online Banking you are allowed to make transfers between your approved Queenstown Bank accounts. You may also make payments to your Queenstown Bank loan accounts. We reserve the right to deny transfers between certain types or accounts under certain circumstances.

A transfer initiated through Business Online Banking before 6:00 p.m. (Eastern Standard Time) on a business day is posted to your account the same day. All transfers completed after 6:00 p.m. (Eastern Standard Time) on a business day or on a Saturday, Sunday or banking holiday, will be posted on the next business day, however, may be available for your use sooner. Our business days are Monday through Friday, except for banking holidays. "Banking holidays" shall mean all federal banking holidays.

The number of transfers from accounts may be limited as described in the applicable portions of the deposit account information. Each payment or transfer through Business Online Banking from a savings or money market account is counted as one of the six limited transfers permitted per calendar month, as described in the Disclosure and Regulations.

If a hold has been placed on deposits made to an account from which you wish to transfer funds, you cannot transfer the portion of the funds held until the hold expires.

You cannot cancel a transfer after it has been entered into the system and the information has been processed and/or transmitted to us.

13. **Bill Pay**

Online Banking Bill Pay services are provided by CheckFree. If you choose Online Banking Bill Pay Service, it will permit you to use your computer to direct payments from your designated online Bill Pay Account to third parties you wish to pay. Through the Bill Pay Service, you can pay bills from your Bill Pay Account to businesses or individuals.

All payments you make will be deducted from the account that you designate as your Bill Payer Account for the Bill Payer Service. Any payments you wish to make through this service must be payable in U.S. Dollars to a payee located in the continental United States. We reserve the right to restrict types of payees to whom payments may be made using the service from time to time. You will not use the Bill Payer Service to make payments to settle securities purchases, payments to interest bearing accounts, tax payments, or court ordered payments.

You agree that the following uses of Internet Banking Service are strictly prohibited. You agree to indemnify, hold harmless, and defend us from and against any and all claims, actions, suits, judgments and expenses (including court costs and reasonable fees of attorneys, accountants and expert witnesses) at your sole expense, arising from your failure to abide by the restrictions. You agree that you will not engage in:

- Unauthorized communication of any charge or credit card information belonging to any other person or entity.
- Unauthorized communication of any information concerning any password or other online access number, code, or identification or any other proprietary information belonging to any other person or entity.
- Use of the Internet Banking Service to copy or distribute or transmit copies of copyrighted materials belonging to any other person or entity except to the extent that the owner has provided express permission to you for such activity. Copying, distributing, or transmitting copyrighted materials other than with permission as specified above is expressly prohibited.
- Communicating any obscene or defamatory information, including but not limited to, computer bulletin boards or in conjunction with e-mail.
- Use of the Internet Banking Service in violation of any telecommunication, postal, or other local or federal laws or regulations, or in the commission of a crime or other unlawful or improper purpose.

When you use Online Banking with Bill Payer, the following terms and conditions apply to you:

- You understand that alimony, child support or other court-directed payments or tax payments are prohibited under this agreement.
- You authorize the bank to make payments to creditors for you as you may authorize (by personal computer) from time to time. You also authorize us to post such payment to your designated bill payer account.
- You understand that we will use reasonable efforts to ensure that payments reach creditors on time, but that we cannot guarantee the time a payment will be posted by a creditor. We will use reasonable efforts to see that creditors reverse any service fee or late charge that is related to a payment process error caused by us. You agree that we will not be responsible for any loss or penalty that you may incur due to lack of sufficient funds or other conditions that may prevent the withdrawal of funds from your primary checking account.
- You understand that National, State, or Regional Networks used to effect transactions may impose fees.
- You agree that any transmission of confidential business or sensitive personal information is at your sole risk.
- There is no limit to the number of bills you can pay.
- If your Bill Payer account becomes inactive for a period of six months, the account will be deleted.

Queenstown Bank of Maryland is only responsible for exercising ordinary care in processing and sending payments upon your authorization in accordance with this Agreement. Queenstown Bank of Maryland will not be liable in any way for damages you incur if you do not have sufficient funds in your Bill Payer Account to make the payment on the processing date, for delays in mail delivery, for changes to the payee's address or account number unless you have advised us of the change sufficiently in advance, for the failure of any payee to correctly account for or credit the payment in a timely manner, or for any other circumstances beyond the control of Queenstown Bank of Maryland. If your Bill Payer Account does not have sufficient funds to make a payment as of the date the transfer or payment is attempted or scheduled to be made, the transfer or payment will be cancelled and no further attempt

will be made by Queenstown Bank of Maryland to make the transfer or payment. Queenstown Bank of Maryland will attempt to notify you by telephone or e-mail, but Queenstown Bank of Maryland shall have no obligation or liability if it does not complete a transfer or payment because there are insufficient funds in your account to process a transaction. In all cases, you are responsible for either making alternate arrangements for the payment or rescheduling the payment through the service.

Users enrolled in Checkfree Billpayer services, also have access to person to person payments via a service known as PopMoney. PopMoney is a secure way to send money or request payments directly from their online banking service using only the recipient's email address.

14. Stop Payment Request

You agree that a Stop Payment Request submitted through Business Online Banking, is submitted in writing for purposes of the Uniform Commercial Code. An Online Stop Payment Request applies to check transactions only. The Stop Payment Request must be received by the Bank in sufficient time to give the Bank a reasonable opportunity to act on it before the Bank pays the item. Depending on the payment method and whether or not the check has cleared, the service will process the request. A Stop Payment Order cannot be released through the Online Banking Online System.

15. Alerts

Your enrollment in the Service includes enrollment to receive transaction alerts and notifications ("Alerts"). Alerts are electronic notices from us that contain transactional information about your Queenstown Bank account(s). Alerts are provided within the following categories:

- Mandatory Alerts provide you with important account notifications, such as information about changes to your Online Banking password, PIN, or login information. You do not have the option to suppress these Mandatory Alerts.
- Account Alerts provide you with notification of important account activities or when certain changes are made to your Service accounts. These Alerts are automatically activated for you. Although you may suppress these Account Alerts, we strongly recommend that you do not do so because they provide important information related to your Service accounts.
- Additional Alerts must be activated by you to be enabled. These Additional Alerts can be accessed from the More menu within Queenstown Bank Mobile Banking.

Account Alerts and Additional Alerts may be managed and/or added online through the Service. We may add new Alerts from time to time or cancel old Alerts. We usually notify you when we cancel Alerts, but are not obligated to do so. Queenstown Bank reserves the right to terminate its Alerts service at any time without prior notice to you.

Methods of Delivery. We may provide Alerts through one or more channels ("EndPoints"): (a) a mobile device, by text message; (b) a mobile device, by push notification; (c) an email account, by an e-mail message; or (d) your Queenstown Bank Online Banking message in-box, by an e-mail message. You agree to receive Alerts through these EndPoints, and it is your responsibility to determine that each of the service providers for the EndPoints described in (a) through (c) above supports the email, push notification, and text message Alerts provided through the Alerts service. Please be advised that text or data charges or rates may be imposed by your EndPoint service provider. Alert frequency varies by account and preferences. You agree to provide us a valid mobile phone number or email address so that we may send you Alerts. If your email address or your mobile device's number changes, you are responsible for informing us of that change. Your Alerts will be updated to reflect the changes that you communicate to us with regard to your primary and secondary email addresses or mobile device number.

Limitations. Queenstown Bank provides Alerts as a convenience to you for information purposes only. An Alert does not constitute a bank record for the deposit or credit account to which it pertains. We strive to provide Alerts in a timely manner with accurate information. However, you acknowledge and agree that your receipt of any Alerts may be delayed or prevented by factor(s) affecting your mobile phone service provider, internet service provider(s) and other factors outside of Queenstown Bank's control. We neither guarantee the delivery nor the accuracy of the contents of each Alert. You agree to not hold Queenstown Bank, its directors, officers, employees, agents and

service providers liable for losses or damages, including attorneys' fees, that may arise, directly or indirectly, in whole or in part, from (a) a non-delivery, delayed delivery, or the misdirected delivery of an Alert; (b) inaccurate or incomplete content in an Alert; or (c) your reliance on or use of the information provided in an Alert for any purpose.

Alert Information. As Alerts delivered via SMS, email and push notifications are not encrypted, we will never include your passcode or full account number. You acknowledge and agree that Alerts may not be encrypted and may include your name and some information about your accounts, and anyone with access to your Alerts will be able to view the contents of these messages.

16. Security

Business Online Banking may utilize a comprehensive security strategy known as multifactor authentication to protect your accounts and transactions conducted over the Internet.

Access IDs and Passwords - One of the main security features protecting Business Online Banking is the unique combination of your Access Identification Code (Access ID), and confidential password.

You determine your Password which is encrypted in our database. Neither this Institution nor its Service Providers have access to this information. Online Banking will automatically deactivate your account after three unsuccessful login attempts within a 20-minute time frame. In this event, you will need to contact Queenstown Bank to provide assistance.

Because your Password is used to access your accounts, you should treat it as you would any other sensitive personal data.

- You should carefully select a Password that is hard to guess.
- You should not use words based on your name, address or other personal information.
- Keep your Password safe.
- Memorize your Password and do NOT write it down.
- You will be required to change your Password every 365 days.
- Your Password should be changed immediately if you suspect that it has been compromised. This can be done at any time from the "Account Services" menu after you log on to Business Online Banking.

Neither this Institution nor its Service Providers will contact you via telephone or email requesting personal information, your Access ID, or your Password. If you are contacted by anyone requesting this information, please contact us immediately.

User Authentication – Your computer is registered with unique identifiers using secure cookies and Adobe® Flash® shared objects to identify your computer and your IP address, and other information to verify your identity. This prevents criminals from logging into your account even if they possess your unique Access ID and password. If your computer is not recognized, the system will require that a security question that was established during your first login be answered correctly prior to continuing.

Encryption – Business Online Banking uses the Transport Layer Security (TLS) encryption technology for everything you do while using Internet banking. Your browser automatically activates this technology when it attempts to connect to our Service. The Service requires a browser that supports 128-bit encryption. The Service will warn you if your browser does not meet this requirement. What this means to you is that your communications are scrambled from your browser to our servers at all times so no unauthorized party can read the information as it is carried over the Internet.

Mutual Authentication – In addition to encryption, Access ID and password, an extended validation (EV) certificate that is in place will populate the browser address bar with a lock icon, providing customers with visual confirmation that they are on a valid website. This provides end to end protection against phishing, spoofing, keyboard logging and other fraudulent attacks without the need for installing new software. EV SSL provides an extra layer of

protection for consumers and website operators by requiring third-party Certificate Authorities (CA) to follow a strict issuance and management process, as defined by the CA/Browser Forum, for certificate approval and delivery.

Cookies - During your use of Business Online Banking, our Internet banking Service Provider will pass an encrypted *cookie* to your computer in order to identify your computer during the session. The encrypted cookie registers your computer with Business Online Banking and your computer will be recognized during future logins. This cookie enables us to process multiple transactions during the session without having to provide an Access ID and Password for each individual transaction. This cookie does not contain any personal information; it simply provides another level of security for our Internet banking product. The cookie is stored on your computer's hard-drive, identifying your computer while you are logged on. When you log off, close your browser, or turn off your machine, the cookie will be destroyed. A new cookie is used for each session; thus, no one can use the prior cookie to access your account.

Additional Security Guidelines:

- All Authorized Users should sign-off after every session; however, online sessions will automatically end after fifteen (15) minutes of inactivity. This is to protect you in case you accidentally leave your computer unattended after you log-in.
- The security of public computers (e.g. in a library, or Internet café) cannot be assured; therefore, we recommend that you refrain from accessing the Service on a public computer.
- Routinely scan your computer, servers, and electronic media using reliable virus detection and anti-spyware products. Undetected or un-repaired viruses or spyware may affect the performance of your computer, corrupt and destroy your programs, files, and even your hardware. Additionally, you may unintentionally transmit sensitive data to another third party or transmit a virus to other computers.
- Keep your computer's operating system and browser fully patched for critical security issues. We recommend use of the most current, fully patched, versions of Internet browsers for accessing Business Online Banking.

17. **ACH ORIGATION**

ACH Origination allows you to initiate PPD/CCD credit and/or debit entries through Queenstown Bank to accounts maintained at the Bank and in other depository financial institutions by means of the Automated Clearing House Network ("ACH") pursuant to the terms of Queenstown Bank's ACH Origination Agreement and the rules of the National Automated Clearing House Association ("NACHA") and Queenstown Bank's operating rules and procedures for electronic entries, including any exhibits or appendices thereto now in effect, or as may be amended from time to time, (the "Rules"), and Queenstown Bank is willing to act as an Originating Depository Financial Institution ("ODFI") with respect to such Entries.

If you apply to originate ACH transactions, we will conduct a risk assessment to determine eligibility. If you are approved to originate ACH entries, you will be required to sign the Bank's ACH Origination Agreement which outlines ACH rules and responsibilities as mandated by the National Automated Clearing House Association (NACHA).

Password requirements for Business Online Banking users who are authorized to submit ACH entries will differ from the password requirements outlined in section 5 of these terms and conditions. Each user will be issued a Go3 Token for added security. This token generates a one-time password that is used to log into Business Online Banking and is needed each time an ACH file is submitted. The password(s) generated by this device is unique to the user account and changes frequently for your protection. One token will be issued to each ACH Originator at no charge. In the event a token becomes damaged or lost, a replacement token will be issued for a \$25.00 fee.

18. **Remote Deposit Capture**

The Remote Deposit Capture service offered by Queenstown Bank is a Remote Deposit Service ("RDS") that consists of a check scanning device, device driver, and access to a browser based software program that permits you to conduct certain check related activities with the Bank electronically. RDS activities include the ability to scan paper checks and electronically transmit to a third-party processor, Fiserv, whose services are available to the Bank, and for Fiserv to use electronic information, including images, captured from these checks to process transactions as Image Replacement Documents (IRDs) as permitted under the Check for the 21st Century Act. The

Services are provided by the Bank and its vendors for access and use by you. There is a monthly fee of \$35.00 assessed to use the Remote Deposit Capture service.

If you apply for the Remote Deposit Capture Service, we will conduct a risk assessment to determine eligibility. If you are approved for the Remote Deposit Capture Service, you will be required to sign the Bank's Remote Deposit Capture Services Agreement which outlines processing rules and responsibilities for the service.

The following is a list of additional hardware and software requirements to use this service:

- Hardware
 - 10GB of available disk space on the system is recommended.
 - 2GB of RAM recommended (1GB minimum).
 - 2.0GHz processor recommended.
- Software
 - Microsoft Windows 7 or higher.
 - Ranger device driver (provided by Queenstown Bank of Maryland).
 - Internet Explorer v11.x.

Password requirements for Business Online Banking users who are authorized to transmit Remote Deposit Capture deposits will differ from the password requirements outlined in section 5 of these terms and conditions. Each user will be issued a Go3 Token for added security. This token generates a one-time password that is used to log into Business Online Banking. The password(s) generated by this device is unique to the user account and changes frequently for your protection. One token will be issued to each user at no charge. In the event a token becomes damaged or lost, a replacement token will be issued for a \$25.00 fee.

ROLES AND RESPONSIBILITIES

Senior Administrators

The Senior Administrator must be authorized to conduct business with us, included as part of your account opening documents or otherwise authorized (or deemed authorized) to act on your behalf, whether under this Agreement or any other agreement with us. You will be required to designate at least one Senior Administrator. You (through the Senior Administrator) then control the Funds Management Services, through the systems available on our website. The Senior Administrator may establish other users (including additional Senior Administrators, Supervisors, Employees, and View Only Employees). You are responsible for any and all Users to maintain the confidentiality of his or her password or login identification and other Security Codes.

The Senior Administrator(s) will be responsible for maintaining your Service settings and User security. Access to your account(s) through the Service will be based upon the identification of Users and authority levels specified by you in your authorization forms. You must notify us if you terminate or wish to change the Senior Administrator. You must also notify us if you add or delete accounts or functionalities.

Senior Administrator responsibilities may include:

- Add, modify, and delete users associated with the client.
- Assign the security level to the user.
- Establish roles for the user (senior administrator, supervisor, employee, view only).
- Establish ability to inquire or add stop payments for the client.
- Choose the electronic documents the user will have access to view.
- Establish which transfer templates the user will be assigned.
- Give access to the user for ACH manager, if applicable.
- Give access to the user for Remote Deposit Capture, if applicable.
- Add, modify and delete transfer templates.
- Add or modify the display groups and nicknames assigned to each account.

The Senior Administrator is responsible for setting up your Users. The Senior Administrator is also responsible for assigning all Supervisors, employees, or other persons with the Security Codes that are necessary to access Services and for establishing what, if any, limitations will apply (including what level of activity is appropriate for each Account). The Senior Administrator changes and maintains your Security Codes.

We will not control or oversee the Senior Administrator function or the activity of Users. You agree to the creation of a Senior Administrator and to all action taken by the Senior Administrator, by any User, and by any person given access to one or more Services by the Senior Administrator or by a User, and all such persons that are your agents for purposes of use of the Services. You further agree to assume all risks associated with providing Security Codes to your Senior Administrator, understanding that this can result in Users and possibly other persons obtaining access to your Account without control or monitoring by us. You must establish authorization parameters and/or limits for each person you authorize to use the Service. You agree to use and implement each control (including template management, verification, access, use of maximum process settings, security, audit and review procedures) to prevent unauthorized persons gaining access to Security Codes or your Accounts.

Supervisors, Employees, View Only Employees:

Supervisors, Employees, and View Only Employees are granted access to Online Banking functions at the discretion of you and your assigned Senior Administrator.

If the approval process is required for various functions it would require authorization from a user with a higher security level than what is assigned to the user. For example, a user with an employee role may have transactions approved by a user with a supervisor role. A user with an employee role will not be able to approve transactions made by a user with a supervisor role.

ADDITIONAL PROVISIONS

1. Bank Liability

We will use commercially reasonable efforts to make all your transfers properly. However, we shall incur no liability if we are unable to complete any transactions initiated by you because of the existence of any one or more of the following circumstances:

- If, through no fault of ours, your Eligible Account(s) and/or Payment Account does not contain sufficient funds to complete the transaction or the transaction would exceed the credit limit of your overdraft account (if applicable);
- Business Online Banking is not working properly and you know or have been advised by this Institution and/or its Service Providers about the malfunction before you execute the transaction;
- If your computer, software, telecommunication lines were not working properly and this problem should have been apparent to you when you attempted the transfer
- The transaction request involves funds subject to hold, dispute, restriction, or legal process we believe prevents their withdrawal;
- We have reason to believe that a transaction request may not be authorized by you or any third party whose authorization we believe is necessary; and/or
- Circumstances beyond control of the Service, our Service Providers, and this Institution (such as, but not limited to, fire, flood, or interference from an outside force) prevent the proper execution of the transaction and we have taken reasonable precautions to avoid those circumstances.

2. Electronic Disclosures

We may deliver amendments to this Agreement and other disclosures to you in an electronic format. Other disclosures may include: monthly account statements, deposit account disclosures, notices regarding changes in account terms and fees, and privacy notices. The requirements to access and view such items electronically is described in the section of these terms and conditions titled, Requirements for Your Use.

With your acceptance below, you agree to accept this agreement and other Online Banking related disclosures in an electronic format. You also agree and represent that you have the necessary equipment for accessing the Service and for viewing electronic disclosures.

You may change the method of delivery at any time (e.g., from electronic format to paper format) of any of the aforementioned disclosures, account statements, or notices. We request that you provide your intent to discontinue electronic disclosures in writing. You may send an email to digitalservices@queenstownbank.com, mail a letter to the address listed below or drop off your written request to any Queenstown Bank of Maryland branch location.

Queenstown Bank of Maryland
Operations Department
PO Box 120
Queenstown, MD 21658-0120
(410)827-8881

You should print or save a copy of all disclosures delivered electronically.

3. Address, E-mail, or Payment Account Changes

When you enroll in Business Online Banking, we may send you a “Welcome” e-mail. We will also send you e-mails and/or secure messages through Business Online Banking regarding important Internet Banking matters and/or changes to these terms and conditions. We will need a valid e-mail address in order to deliver this information to you.

It is your sole responsibility to ensure that your contact information is current and accurate. This includes, but is not limited to, name, address, phone numbers, and e-mail addresses. Changes to your email address can be made by the assigned Senior Administrator or by contacting our Operations Department at (410) 827-8881. Other changes to your account must be made in person at any Queenstown Bank of Maryland location.

4. Service Termination, Cancellation, or Suspension

In the event you wish to cancel the Service, please contact our Operations Department at (410) 827-8881.

We may terminate or suspend the Service to you at any time. Neither termination nor suspension shall affect your liability or obligations under this Agreement.

Access to Business Online Banking may be canceled in whole or part without prior notice due to insufficient funds in one of your accounts or other circumstances that may create an unanticipated liability to us. If your account(s) is closed or restricted for any reason, or if there has not been any Internet Banking activity for a period of 6 consecutive months, accessibility may automatically terminate.

After termination or suspension of Business Online Banking, we may consider reinstatement once sufficient funds are available in your accounts to cover any fees and other pending transfers or debits. In order to request reinstatement of the Service, call our Operations Department at (410) 827-8881.

5. Governing Law and Relation to Other Agreements

Accounts and services provided by this Financial Institution may also be governed by separate agreements with you. This Agreement supplements any other agreement(s) and/or disclosures related to your Account(s) and provided to you separately.

This Agreement shall be governed by and construed in accordance with federal laws and the laws of the State of Maryland.