ONLINE BANKING SERVICES AGREEMENT

This agreement ("Agreement") describes your rights and obligations as a User of the Online Banking (OB), Bill Payment, MX, internal transfer, external funds transfer, Mobile Banking, mobile remote deposit capture (mRDC), or Text Banking Services (collectively, "Services"). It also describes the rights and obligations of Apple Bank for Savings (Apple Bank or Bank), a New York state-chartered savings bank. Please read it and make a copy for your records. Definitions and abbreviations appear in Section XVII.

By subscribing with your Electronic Signature, requesting access or using the Services (i.e., by clicking the I Accept button), you (and anyone else you authorize) agree to comply with, and be bound by, this Agreement, any Addenda thereto, applicable law and regulations, the Operating Rules and Guidelines of NACHA The Electronic Payments Association (NACHA) and the Bank's rules, regulations, policies and procedures, including amendments made from time to time (Rules).

You warrant that you: (1) are over the age of 18 and all information you provide us through electronic communications (ECs) or otherwise is, and shall continue to be, true, correct and complete, (2) will not impersonate anyone or use any name or personal information belonging to another, (3) will not use the Services for any unlawful or prohibited purpose (e.g., internet gambling), (4) will not copy, store, use, recreate, modify or interfere with any intellectual property and related rights of the Bank or any Third-Party Provider of information or Services hereunder, including, but not limited to, rights related to trademarks, service marks and copyrights (IP), and (5) will not use the Services in any way that could damage, disable, overburden, or impair or interfere with another's use and enjoyment of them.

I. ONLINE BANKING SERVICES OVERVIEW

A. Account Access

You may access or view your Eligible Accounts through the Online Banking (OB) Service. Upon Enrollment in the Bill Payment Service at least one Eligible Account must be a primary checking account to be used for payments. Upon Enrollment in the External Funds Transfer Service, any External Account(s) you choose to link to your Account(s) must be owned or controlled by you. Accounts registered through the MX Service must also be in **like titled ownership**.

Upon your Initial Login to the OB Service you will receive a Secure Access Code (SAC), a randomly generated one-time multi-factor authentication code used as an enhanced security measure intended to further confirm your identity as the true User or Authorized Person having authority to access the Service. The SAC will be delivered as an email, phone or cell number (as a text message), i.e., the SAC.

B. MX Service

The MX Service allows you to view your accounts held at multiple U.S. financial institutions (FIs), from within the OB Service. You can consolidate, organize and present certain information from your accounts at the Bank and other FIs, such as banks, credit unions, brokerages, credit card providers, billers and other sources of financial information (Information Providers) on secure web pages. The Service includes the following features:

transaction categorization, account aggregation, data visualization, cleansed transaction descriptions and widgets.

To provide the features included in the MX Service we must access third party Web sites and databases containing your financial account information. The Bank regards your privacy and security with utmost importance and is committed to safeguarding any information that you share with us. For each of your registered accounts at other FIs, you will need to provide your User ID, Password, account number and/or personal information number (PIN), Secure Access Code (SAC) or other Login Credentials before information could be retrieved, as applicable from your Information Providers.

C. External Funds Transfer

Upon Service enrollment, and registration of accounts, you will be eligible to set up external accounts for use of the External Funds Transfer Service. "Electronic Funds Transfers" or "EFTs," defined at Section XVII.

To Enroll, register and use the External Funds Transfer Service:

- First, you must furnish and submit the American Bankers Association (ABA) Routing Number and account number for each such External Account designated to be linked; and
- Second, you must verify two small micro-deposits and withdrawals (less than $1.00) that will be made to the account.

Once you have confirmed the micro-deposits and withdrawals, the registered External Account will be linked for immediate display to allow you to schedule an external funds transfer, allowing you to initiate Electronic Funds Transfers through an Automated Clearing House (ACH) Network. Within certain limitations, you will be able to initiate External Funds Transfers to come from (debit) or to go to (credit) your External Accounts. For further details, see the External Funds Transfer agreement upon registration.

D. Bill Payment Service

You may set up Bill Payees and schedule one-time, future or recurring payments through the Bill Payment Service (See, Section III, below).

E. Internal Transfers

You will be able to effect internal funds transfers among your Eligible Accounts at Apple Bank through the OB Service, with certain limitations. For instance, retirement accounts (e.g., IRAs, QRPs, etc.) and certain accounts held in a fiduciary capacity may not be Eligible Accounts for internal transfers or Text Banking.

.

G. Mobile Banking

OB Users can access all Service features through a mobile device, smart phone, personal digital assistant, tablet or other hand held device (Mobile Device) using the Bank's mobile banking application provided by Q2 Software, Inc. (Q2), downloadable at the Apple iTunes Store or at Google Play. At present, Q2mobility applications are operable using Apple/iOS iPads and iPhones and Android tablets and smart phones, Apple iOS and Android OS. NOTE: Mobile carrier text and data fees may apply.

Generally, the following OB Services will be available from a Mobile Device by clicking on the Mobile Banking button, Logging In and following the prompts:

1. Enroll in OB
2. View account balances and histories
3. Make Bill Payments to existing Payees
4. Create new Bill Pay Service Payees
5. Conduct permitted internal funds transfers between your linked Apple Bank accounts
6. Create or initiate External Funds Transfers
7. Aggregate financial account information (through MX Service)
8. Make other Account Services Changes
9. Touch Authentication Login
10. Text Banking
12. Send and receive messages securely within an OB session, using the Message Center
13. Access our Mortgage Loan Service to view your existing mortgage loan information

Touch Authentication

The identity of each customer using the Mobile Banking application will be verified using multi-factor authentication and layered security measures. Upon activation, Touch Authentication functionality is available for Login purposes to customers electing to use that feature and, in such instances, the User identity authentication process will occur using accepted biometric identification methods.

Text Banking

Upon activation, Users may enable the text banking feature of mobile banking, by which certain basic account information (e.g., balances, etc.) can be quickly retrieved, even without the formal Login process, through your registered Mobile Device. Mobile carrier message and data fees may apply. Users may later opt out or disable the Text Banking feature within the application. For further details, see the Text Banking Service Addendum hereto.

Mobile Banking Security

Mobile banking involves the same risks that OB ordinarily entails. But Users of Mobile Devices take additional risks by using them wirelessly in public places, possibly in proximity

to wrongdoers or malefactors seeking to steal personal data and information, personally or using electronic devices. Such circumstances call for Users to exercise even extra caution when conducting any banking business or transaction from a Mobile Device in a public place, to reduce the risks.

For those reasons, Users should be on high alert to their surroundings, nearby persons and devices. Further, Users must remember to always verify the appearance of the landing page, and prior Log In date and time, every time BEFORE logging in to OB from a Mobile Device.

H. Mobile Remote Deposit Capture Service (mRDC Service)

The mRDC Service is available upon separate Enrollment, upon agreement to the mRDC terms and conditions.

The Service provides Users with the ability to quickly and conveniently deposit paper checks to their accounts at the Bank, electronically capturing each check image and related data, and transmitting the same to the Bank for processing and collection, through use of a Mobile Device. The Service is afforded through Ensenta Corporation, a Third-Party Provider. For further details, see the mRDC Service Addendum hereto.

I. Customer Identification

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all FIs to obtain, verify, and record information that identifies each person who opens an account. What this means for you: when you open a new account or enroll in any of the Services, we reserve the right to ask for your name, address, date of birth, social security number, department of motor vehicles license registration number and state, and other information that will allow us to identify you.

Credit reporting agency and government database information may be utilized in verifying your identity. By clicking on the I Accept button and submitting the OB and/or related Services applications through ECs, you consent and authorize the Bank, Q2 Software, Inc. (Q2), Fidelity National Information Services, Inc., its subsidiaries and affiliates, (collectively, FIS Global), PNC Bank, N.A. (PNC Bank), MX Technologies, Inc. (MX), Ensenta Corporation (Ensenta), IDology, Inc. (IDology) and their subsidiaries, affiliates, and third-party processing agents (i.e., collectively, Third-Party Providers) to access your credit report and government database information in accordance with the Fair Credit Reporting Act (FCRA) and other applicable law, for purposes of ascertaining your identity, determining eligibility and using it to enable you to enroll, access and use the Service. The requested information may include non-public personal information about you and concern your property, finances or credit.

The entities referenced above may also:

(1) pose a series of other security questions that must be satisfactorily answered,
(2) require your verification of micro-deposits and withdrawals to External Accounts, and, possibly,

(3) to perform a live Login in real time to access your account(s) on the website(s) of another FI (e.g., submitting your User ID, Password, etc.) and/or
(4) submitting written proof of your ownership of the Accounts.

Only identified applicants qualify to Enroll, register, activate and/or use of OB or any of its Services.

J. Power of Attorney

Upon application for OB Access and approval by the Bank if all criteria are met, a duly appointed attorney-in-fact (Agent) may be recognized as an Authorized User of one or more Services having the requisite legal authority to perform services on behalf of the Principal.

A **separate** Agent profile must be set-up in our system apart from the Principals User Profile. User ID and Password is required and will be established by the Bank upon approval.

Should Agent also be (or become) an individual Apple Bank account holder, he/she agrees that **his/her own profile**, user name and password must be used for those purposes. The Agent further promises that actions performed in that capacity, i.e., as a fiduciary for the Principal under the POA, will be kept separate and apart from those of the individual; there can be no commingling of funds.

II. PAPERLESS DELIVERY OF STATEMENTS (E-STATEMENTS) AND NOTICES OF CHANGE; UPDATING EMAIL ADDRESSES

(1) e-Statements

Upon enrollment into Online Banking, you are agreeing to delivery through e-Statements and, therefore, will not receive periodic Account statements on paper by ordinary mail. Instead, Users will receive them through electronic communications (ECs).

The paperless delivery of e-Statements will occur through secure posting of them on in Online Banking (monthly or quarterly, depending on the Account type and activity). Upon such posting, delivery of e-Statements is considered complete. The Bank may treat an invalid or malfunctioning e-mail address as a withdrawal from receiving paperless periodic statements.

In most cases, if you do not want to continue receiving paperless delivery of your statements, i.e. e-Statements, you may opt-out, using the OB Service, through which you submit a request to discontinue paperless delivery, on a per account basis. However, if you currently have combined statement accounts for e-Statement delivery, you must visit an Apple Bank branch location or contact CustomerLine, directly, if you want to change your account statements combinations or e-Statement delivery status.

(2) e-Delivery of Notices via Email

The Bank reserves the right, upon prior notice to you, to provide you with the following documents through ECs: (A) Notices of Change(s) regarding agreements, terms, conditions

and disclosures for your Eligible Account(s) and the Services (e.g. changes in services, charges and fees, time frames, funds availability, etc.), as well as (B) Notices of Renewal of CDs, etc. Delivery of notices of change may be made via email to your email address on record with the Bank, rather than through hard copies via ordinary mail.

(3) Update Email Address

Your email address on file with the Bank must be kept current. When your information is changed, you must promptly update it to ensure proper communications with us about important security matters [e.g. Password changes, User ID changes, email address changes (to new and old addresses), adding new Bill Payees, etc.]. You may do so securely through the OB Service. First, Log in to OB. Then, simply navigate to the appropriate page link on Change Email Address and update it. Changes will be effective when processed by us.

III. BILL PAYMENT SERVICE

A. Description of Service

The Bill Payment Service allows you to use a Computer or Mobile Device to direct payments from your Payment Account (i.e. a primary checking account), on a one-time or periodic (recurring) basis, to payees that you designate, subject to the limitations, terms and conditions of this Agreement and any agreement with the Q2s third-party service provider Fidelity National Information Services, Inc., its subsidiaries and affiliates, (collectively, FIS Global). There is no monthly service fee for the Bill Payment Service.

Bill Payments are:

(1) scheduled and made through Payment Instructions given by you,

(2) deducted from the Payment Account, and

(3) payable in U.S. dollars to a payee located in the continental United States. With certain limitations, you can make payments to businesses or individuals.

B. Prohibited Payments

The Bank reserves the right, from time to time, to restrict the types of payees to whom payments may be made using the Service. You may not use the Bill Payment Service to settle securities purchases, payments to interest bearing accounts, tax payments or court ordered payments. The sole responsibility for making any such payment(s) if they are delayed or are processed or credited improperly for any reason will be yours. Among others, we will not process payments meeting any of the following criteria:

- Designated by the Office of Foreign Asset Control as being a prohibited payee
- Having an address outside the United States (except for APO)
- Court ordered payments such as alimony, child support, speeding tickets, etc.
- Tax entities
- Collection agencies

- Payments prohibited under the Unlawful Internet Gambling Enforcement Act (UIGEA), 31 U.S.C. 5361 et. seq.

If a payment to a prohibited payee is inadvertently processed, the Payment Guarantee outlined below does not apply to that payment, and we reserve the right to not process a payment to that payee in the future.

C. Bill Payment Limits

Standard. You may not schedule any individual Bill Payment in an amount greater than $15,000.00 and, in the aggregate on any one (1) business day, more than $100,000.00.

Commercial. Bill Payment for commercial customers may not exceed $25,000.00 per transaction, nor, in the aggregate on any one business day, more than $250,000.00.

D. Order of Payments

On any Send On Date, Bill Payments will be processed pursuant to your Payment Instructions, as scheduled (at sessions end). FIS Global may process your Payment Instructions in one of two ways:

(1) as checks drawn against your Account, or

(2) as items processed electronically through EFTs.

For Bill Payments processed through EFTs, FIS Global will post an electronic debit against your Account on the Send On Date, in the Payment Amount, for each scheduled Bill Payment. For those processed as checks against your Account, the item will be paid in the order received by the Bank.

For general information pertaining to ACH/EFT & Check Payment Order, please refer to the About Your Apple Bank Accounts brochure and the Account Disclosure pertaining to your account(s).

E. Payment Instructions

Sufficient funds **must** be available in your Payment Account on each scheduled Send On Date to fund the cost of each item to be paid. You may elect to schedule payments to recur in the same amount at regular intervals. Your Payment Instructions must be accurate. If you attempt to initiate a Scheduled Payment Date that falls on a non-business bay (i.e. Saturday, Sunday or legal holiday), an alternate available date will be offered for you to select as the Send On Date. Once funds are withdrawn from the Payment Account we may make the payment(s) by EFT or by mailing a check(s) to the payee(s).

F. Scheduling Payments

When scheduling Bill Payments, be sure to provide enough time between the Delivery By date and the due date of your bill. Payments to electronic merchants (Payees) must be scheduled two (2) Business Days before the payment due date. For merchants that cannot accept electronic payments must be scheduled five (5) business days before the due date. For

further information about Scheduling Bill Payments, go to the Bill Pay Tab during your OB session and click on the Help button.

G. Send On Date vs. Deliver By Date

Always note the difference between the Send On and Deliver By dates. The Send On date is the date we will attempt to deduct the payment from your Payment Account. If the attempt fails because you did not have sufficient funds in your Payment Account you, alone, will be responsible to reschedule the Bill Payment (which could not occur) or to make alternative arrangements to fund and make the Payment.

Following a failed attempt due to NSF or uncollected funds the Bill Payee may present an ACH a second time to receive your payment. You will receive an in-session or Message Center message advising you of any failed Bill Payments returned for such reasons and you will be charged an NSF fee of $35.00. You may also need to reschedule your Bill Payment.

If you schedule a payment with the Send On Date as the current date, you must have sufficient available funds in your account at the time the payment is scheduled. The funds will be deducted after you Log Out of the session. If you schedule a payment with the Send On Date in the future (and Payment Instruction will be stored), you must have sufficient available funds in your account when we attempt the deduction. This can occur anytime between 12:01 am and 4:00 pm ET.

The Deliver By date is the date that you can expect the payee to receive your payment. The Deliver By date for your payment should be no later than the due date the payee has indicated for the payment.

H. Customer Drafts. If a payee cannot accept an ACH, the Bill Payment Service will send a draft drawn against your account, which may take up to seven (7) Business Days.

I. Adding Payees. When you add a new payee, it may take two (2) Business Days to finalize the setup of a new payee. Therefore, you should schedule any payment to a new payee no later than four (4) Business Days before the next anticipated due date [i.e. as provided by agreement with the payee (ignoring any grace period) or as shown on its statement/invoice], to allow adequate time to set up the payee and verify information about your Account with the payee.

J. Payment Guarantee

If a properly scheduled electronic payment is not received and posted on time by the payee, FIS Global will attempt to remove any late fees or assessed finance charges. (Finance charges are calculated based on your payment amount rather than your entire balance.) If the payee is unwilling or unable to remove them, FIS Global will pay the fees and finance charges directly to the payee. In addition, FIS Global will attempt to add a note of explanation to your account to ensure that the situation does not negatively impact your credit rating.
The Payment Guarantee applies to late fees and/or finance charges associated with the late posting of a payment, provided that the following conditions are met:

1. You scheduled the payment to be delivered on or before the due date of your bill, excluding any grace periods.

2. The payment was not made to a prohibited or excluded payee(s) (see below):

- Payments to payees outside of the United States Payments
- Payments to payees located in the Armed Forces Postal Codes, such as AE & AP
- Payments that failed due to insufficient funds or other reasons
- Payments to settle securities transactions
- Payments to payoff special or delayed financing for purchases
- Court-ordered payments such as alimony, child support, speeding tickets, etc.
- Payments to credit counseling agencies who pay creditors on your behalf
- Payments to Tax agencies
- Payments to collection agencies
- Payments prohibited under the Unlawful Internet Gambling Enforcement Act (UIGEA), 31 U.S.C. 5361 et. seq.

3. The information you supplied is correct (i.e. the payee name and address; your name and account number as it appears on the payee's records).

4. Your Payment Account had sufficient funds during our first deduction attempt on the Send On date.

FIS Global will only be responsible for the direct fees or finance charges associated with the late payment. It will not be responsible for any other consequential damages that might arise from the late payment.

K. No Duty to Monitor Payments; Bank Liability. The Bank is responsible only for its acts of gross negligence or willful misconduct in the processing and sending of payments upon your authorization (see also, Sections IV and XI, herein). In no event will the Bank be liable for monetary damages you incur because of:

- Insufficient available or collected funds in your Payment Account to make the payment on the processing date.
- Delays in mail delivery.
- Changes to the payee's address or account number (unless the Bank has been advised sufficiently in advance of the change to timely process the payment).
- The failure of any payee to correctly account for or credit payment(s) in a timely manner, or
- Any other circumstance beyond the reasonable control of the Bank.

If the Online Service session during which you schedule a Bill Payment or place an EFT ends by 12:00 PM ET, the Bank will be considered to have received it on that day. If not, it will be considered received on the following Business Day. For entries made using the Service, the time recorded by us shall be deemed the official time of the transaction.

If your Payment Account does not have available funds sufficient to make a payment as of the date the payment is debited to your Account, we may block the Bill Payment Service until the Payment Account has sufficient funds. In such event, the Bank may attempt to notify you by e-mail or U.S. Postal Mail, but it will have no liability to you if it cannot complete a payment because there are insufficient funds in your Payment Account to process it. You are solely responsible to contact the Bank at (914) 902-APPLe (2775) to make alternate arrangements or to reschedule any payment not processed. In the case of fixed payments, only the payment currently scheduled will be impacted. Fixed payments scheduled for future dates will not be affected.

L. Cancel or Change Payment Instructions. You may cancel or change an outstanding Bill Payment using the Service prior to 9:00 AM ET on the Business Day that the processing of the transaction is scheduled to be initiated, i.e. the Send On Date. If you ask us to cancel a payment after it has been issued and we agree to do so, we may charge you a stop payment fee. Oral stop payment orders will only be effective for a period of fourteen (14) days. You must confirm any oral stop payment order in a signed writing before that time elapses. After six (6) months, any confirmed stop payment order will terminate and must be renewed in writing to continue in effect. The Bank may pay any item presented following the lapse of any stop payment order.

The Bank may cancel a Bill Payment in good faith if we believe it might be fraudulent. In such an event, the Bank will attempt to contact you to inform you.

You may cancel a recurring transaction by verbal or written no later than three (3) Business Days before the Send On date of the transaction by contacting CustomerLine at the address or phone number listed below (see Section IV. C.). If you call, CustomerLine will be authorized to act on your instructions once it has authenticated your identity through the Bank's internal procedures. The Bank may also require you to put your request in writing and provide it to us within 14 days. The notice must detail whether the cancellation applies to only one of the recurring transactions, or all transactions in the recurring stream

M. Multiple Person Bill Payment Accounts. If more than one person has access to a Payment Account, each one may individually enroll in the Bill Payment Service. Each person needs a unique Password, but may choose to use the same payee list. An individual may terminate her/his Enrollment in the Bill Payment Service without affecting the Service for any other person Enrolled in that Payment Account. However, any one of them may terminate Service, which will terminate it for all Enrolled persons on the Payment Account for any reason.

IV. CONSUMER ELECTRONIC FUNDS TRANSFER (EFT) PROVISIONS

A. Scope. These provisions apply to any EFT conducted through the OB, MX, Bill Payment, internal transfer, External Funds Transfer, Mobile Banking, or Text Banking, or any other Service(s) available now or hereafter by which you authorize and instruct us or some other FI, through Q2, Fidelity National Information Services, Inc. (FIS Global), and the originating depository financial institution (ODFI), or any third-party processor and any ACH network, to debit or credit one or more of your deposit Accounts. The Act and CFPB Reg. E, as defined herein, govern consumer EFTs. The Bank may rely on any exceptions or exclusions to the provisions contained in the Act or Reg. E. Any terms not defined herein but which are defined in the Act or Reg. E shall have the same meanings as in said statute and

regulation. For purposes of this section, Apple Bank's Business Days are Monday through Friday, excluding holidays.

B. Your Liability. The rules set forth below determine your liability for any unauthorized EFT or any series of related unauthorized EFTs:

1. If you permit other persons (i.e. Authorized Persons) to use your User ID, Password or other Login Credentials for access to OB, MX, Bill Payment, internal transfer, External Funds Transfer, Mobile Banking, mRDC, Text Banking, or other Service(s) hereunder, you are responsible for any Account access, activity, transfers or transactions they make, schedule, initiate, perform, authorize or direct.

2. You should notify us **immediately** if you believe your User ID, Password or other Login Credentials are lost, stolen or known to someone other than yourself, and/or you believe that someone has effected (or may effect) an unauthorized EFT (e.g. an electronic funds transfer money from any of your accounts or External Accounts; a payment from your Payment Account; or a P2P money transfer without permission, etc.). Telephoning is the best way of keeping your possible losses to a minimum.

3. Call the Bank **immediately** at (914) 902-APPLe (2775) if you suspect any unauthorized or fraudulent activity on your Account. **For 24 hour/day reporting of lost or stolen cards, select option 8.**

4. If your periodic statement shows any EFT transaction that you did not make, you must tell us AT ONCE. If you do not notify us within sixty (60) days of transmittal of the FIRST statement showing one, you may not get back any monies you have lost after the sixty (60) days, if we can prove that we could have stopped someone from effecting the unauthorized EFT transaction(s) if you had told us in time. Our liability cannot exceed the amount of the unauthorized EFTs that occurred within the 60-day period. If a good reason (such as a long trip or a hospital stay) was the reason that you did not know of the loss, theft or compromise of your Password, we may extend the time in our discretion.

We will notify you with the results of the investigation within ten (10) Business Days after we hear from you and will correct any error promptly. If more time is needed, however, we may take up to forty-five (45) days to investigate a complaint or a question related to a transaction. If this occurs, we will credit your Account within 10 Business Days for the amount you think is in error. This will allow you to use the money during the time it takes us to complete our investigation. If an alleged error involves an EFT outside a state or territory or possession of the United States, the applicable time periods for action by us are twenty (20) Business Days (instead of 10) and ninety-(90) calendar days (instead of 45). If we determine that no error occurred, we will send you a written explanation within three (3) Business Days after the investigation is complete. You may request copies of the documents that were used in the investigation.

These limits on your possible liability for losses due to unauthorized EFT activity on your Accounts or Payment Account may not apply, to the extent permitted by law, if

the Bank determines that you participated in fraudulent conduct in the handling of your User ID, Password or other Login Credentials.

You may notify the Bank verbally, by telephone, or in writing. Notification by general e-mail to report an unauthorized transaction is not secure and, therefore, not advised.

C. Errors, Omissions or Questions. If you believe there are errors or omissions on your periodic statement, an EFT receipt or confirmation, or if you have any questions regarding your OB, internal transfer, Bill Payment, Mobile Banking, or external funds transfer Services or transactions,

Call CustomerLine, at (914) 902-APPLe (2775), or write us at:

Apple Bank for Savings
c/o CustomerLine
900 Stewart Ave
Suite 605
Garden City NY 11530

For questions related to specific transactions which you believe may not have been authorized please call (800) 216-6985.

We must hear from you at the telephone number or address, listed above, no later than sixty (60) days after we sent you the FIRST statement on which the problem or error appeared. We will need:

1. Your name and Account number;

2. A description of the error or the transfer in question and an explanation concerning why you believe it is an error or need more information; and

3. The dollar amount of the suspected error and date on which it occurred

V. NO HANDWRITTEN SIGNATURES ARE REQUIRED

When any Bill Payment, MX, internal EFT, External Funds Transfer, Mobile Banking, mRDC, Text Banking, or other OB Service generates a payment item(s), fee(s) or charge(s) against your Account, you agree that we may debit your Payment Account or other Account without requiring a physical signature on the item or other instruction. The mere use of the User ID and Password is legally sufficient for such purposes.

VI. ELECTRONIC MAIL (E-MAIL)

If you send the Bank an e-mail message, it will be considered received on the following Business Day. You may NOT use or rely on e-mail messaging to report a claimed error or an unauthorized or disputed transaction from one of your Accounts or if you need to stop a payment that is scheduled.

NOTE: The Internet (i.e. from outside of the Apple Bank OB portal) is **NOT** secure for sending email messages. Do not send any sensitive or private information (e.g. SSN, account number, account information, User ID, Password or other Login Credentials etc.) to the Bank via any Contact Us form on the Apple Bank Website, or any general or public e-mail messaging system.

You should **ONLY** provide private or sensitive information to the Bank when it is encrypted (through SSL) or sent directly and **SECURELY**. This can be done through the OB Service, following the instructions and prompts.

Update Email Address. It is very important that you provide and keep your email address on file with us current. See Section II. (3), above.

VII. PROFILE LINKS

Together, your tax identification number (TIN or SSN) and designated customer profile will determine which Eligible Accounts may be linked to OB, Bill Payment, External Funds Transfer, Mobile Banking, mRDC, and Text Banking Services. Profile linked Accounts will appear together without regard to ownership. Consequently, you or an Authorized Person could view all your linked Accounts, including joint, custodial (e.g. UTMA accounts), retirement accounts (e.g. IRAs; QRPs) or certain business accounts (e.g. sole proprietorship). However, access to such accounts for certain transactional purposes (e.g. Bill Payments, EFTs, Text Banking, etc.) may be prohibited.

Whenever any of the Linked Accounts that you register under any of the Services (i.e. OB, Bill Payment, External Funds Transfer, Text Banking, etc.) is a joint account, your use of the Services shall be deemed to confirm that your joint account holder(s) has or have consented and authorize you to use the Services. We will end your use the Services if any joint account holder notifies us that (i) they never consented to your use of the Service, (ii) the joint account can no longer be operated on your instructions alone, or (iii) they are withdrawing consent for you to operate the joint account.

VIII. OTHER ACCOUNTS

If you are a business, fiduciary or other entity, any User of any of the Services, directly or through an Authorized Person, on such terms, conditions and agreements as we may require, shall be and hereby is authorized to:

- Enter into this Agreement and any Addenda thereto, as amended from time to time;
- Access each of your Accounts as are available through the Services for viewing, transactional or any other purpose(s); and
- Use the OB Service for any purpose available through the Services.

IX. TERM AND TERMINATION

A. Term. This Agreement will become effective on the Effective Date and shall remain in full force and effect until termination, as follows:

B. Termination for Cause. We may immediately terminate any or all OB Services without prior notice to you, if or when you:

1. Do not pay when due any required fee(s); or
2. Do not comply with the agreement(s) governing your Accounts; or
3. The Accounts are not maintained in good standing.

The Bank will promptly notify you if, for any reason, we terminate this Agreement or your continued access to Services.

C. Termination for Convenience. To terminate this Agreement, you must notify the Bank and provide your name, address, the Service(s) you are discontinuing, and the termination date of the Service(s). When Bill Payment Services are terminated, any pre-scheduled Bill Payments may also be cancelled. You may notify the Bank of your intention to terminate by any of the following methods:

- By sending a request to the Bank through the secure messaging center of the OB Service
- By calling CustomerLine at (914) 902-APPLe (2775)
- By writing a letter and either sending it to the following address: Digital Banking Services, c/o Apple Bank 900 Stewart Ave Garden City, NY 11510, or giving it to a Customer Service Representative at any of the Bank's locations.

The Bank may terminate any Service for its convenience, in its discretion, at any time and for any reason. If it does, it will attempt to notify you in advance, but is not obliged to do so.

D. Termination for Inactivity. If you do not: (A) Log In to your Online Account, or (B) schedule and effect any transaction(s) on your Payment Account during any consecutive 90-day period, we may convert your Online Account and/or Payment Account to inactive status. If the Bank considers them inactive, you will need to contact us to re-activate the Services before you will be able to access information, make transfers or schedule any transactions.

X. FEES

OB Fees. The Bank offers you the regular benefits and convenience of OB, Bill Payment and External Funds Transfer Services **with no monthly Maintenance Charge**. The standard fees and charges applicable to your Accounts, as set forth in Maintenance and Service Charges, continue to apply.

Apple Bank's Fees and Service Charges. Maintenance and Service Charges specifically associated with any account are set forth in the Account Disclosures you receive at the time of account opening.

XI. LIMITED LIABILITY OF THE BANK AND THIRD-PARTY PROVIDERS

A. Our Liability. This Section explains the Bank's and Third-Party Providers liability to you only to the extent that the Agreement, Addenda, notices or other disclosures do not separately disclose it. In the event of a conflict, the pertinent provisions of the Addenda shall govern.

B. **IMPORTANT:** Upon successful Login to the Services **by anyone** using your User ID, Password, other Login Credentials or any other authentication control, the Bank and its third-party vendors or processing agents may rely and act upon any information and/or instructions received.

In the event of any unauthorized use of your Login Credentials or personal information, **you will be liable** for the resulting losses **unless** you provide the Bank with prompt notice of the theft, loss, misappropriation or possible breach of your Password or any of your Login Credentials and, notwithstanding such notice, the Bank or its Third-Party Providers (defined at Section XVII) mishandle your notification and request to block any further use of the Services as a result of **gross negligence, willful misconduct or breach of an explicit representation or warranty** set forth herein.

C. The Bank and Q2, FIS Global, PNC Bank, MX Technologies Inc. (MX), Ensenta, , IDology and their subsidiaries, affiliates and third-party vendors or processing agents (Third-Party Providers) may rely on the information you provide through OB, MX, Bill Payment, External Funds Transfer, Mobile Banking, mRDC, or Text Banking Services.

D. The Bank and Third-Party Providers **will not be liable** to you for delays or any failure to provide uninterrupted access to OB, Bill Payment, MX, External Funds Transfer, Mobile Banking, mRDC, Text Banking, , other Services or Accounts. Unless otherwise required by law, we and they are only responsible to perform Services as described in this Agreement or the Addenda thereto. We and they may **ONLY** be liable for the actual amount of direct loss or damage that you sustain that directly results from gross negligence, willful misconduct or the breach of an explicit representation or warranty set forth herein.

E. Regarding Bill Payment Services, FIS Global may be liable to you pursuant to its Payment Guarantee (see Section III. J., above).

F. In addition, we and they will not be liable to you in the following instances:

1. If you provide any incorrect, misleading, incomplete or unauthorized information, or withhold any required information, regarding any of the Services provided pursuant to this Agreement or Addenda thereto.
2. If through no fault of the Bank, you do not have sufficient available funds in your Account(s), Payment Account and/or External Account(s) to make or fund a scheduled Bill Payment, an External Funds Transfer, or a Text Banking transfer.
3. If the Q2 technology platform temporarily fails and/or any one or more of the Services, your operating system or software is not functioning properly at the time you access them or attempt to initiate a transaction.
4. If any FI holding your External Account(s), Third-Party Provider or an ACH Operator or network provider mishandles, prevents or otherwise delays the processing or posting of any Bill Payment, External Funds Transfer, Text Banking or P2P transfer, except as otherwise provided for herein.

5. If circumstances beyond the control of the Bank and/or Third-Party Providers (such as fire, flood, power outage, equipment or technical failure or breakdown) prevents an EFT transfer or other Bill Payment transaction from occurring despite reasonable precautions that we have taken.
6. If there is an administrative hold on your Account(s), Payment Account or External Account(s) (e.g., if access to or use of them is blocked in accordance with the Bank's Rules, NACHA Rules or other FI rules, applicable law or regulations).
7. If there is an outstanding item of legal process resulting in a hold against your Account(s), Payment Account or External Account(s) including, but not limited to, restraining notice, execution, sheriffs or marshals levy, IRS Notices of Levy, NYS Tax Compliance Levy, Levy by execution, Court Ordered restraint, attachment, warrant or seizure notices, etc.).
8. If your funds are subject to a legal proceeding, injunction, lien or other encumbrance restricting a Bill Payment, External Funds Transfer, Text Banking or P2P transfer.
9. If your Bill Payment, EFT, Text Banking or P2P transfer authorization terminates by operation of law.
10. If your Account transfers exceed federal transaction limitations.
11. If you believe someone has accessed one of your Accounts, Payment Account or External Accounts without your permission and you fail to **IMMEDIATELY** notify the Bank (and any affected third-party FI in an external funds transfer).
12. If you have not properly followed the instructions on how to make an External Funds Transfer, or to schedule or make a Bill Payment, mobile remote deposit capture, (mRDC) or Text Banking.
13. If you provide erroneous, misleading, incomplete or unauthorized information or instructions to or withhold correct information from the Bank, Q2, FIS Global, PNC Bank, MX, Ensenta, , IDology or their subsidiaries, affiliates or third-party vendors or processing agents (Third-Party Providers).
14. If we have receive and act upon erroneous, misleading, incomplete or unauthorized or instructions including, but not limited to, name(s), dollar amount(s), account numbers, ABA bank routing numbers, email addresses, phone numbers, etc.
15. If we have a reasonable basis for believing that unauthorized use of your User IDs, Passwords, Login Credentials, Secure Access Codes, one-time passwords, Account(s) or any of the Services has occurred, are threatened or may be occurring
16. If you default under this Agreement, any Addenda thereto or other agreements with us, or
17. If you or we terminate this Agreement.

THE FOREGOING SHALL CONSTITUTE THE BANK'S AND THIRD-PARTY PROVIDERS ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY. IN NO EVENT SHALL WE OR THEY HAVE ANY LIABILITY TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES RESULTING FROM OR ARISING OUT OF THIS AGREEMENT OR ADDENDA THERETO.

NO WARRANTIES. THE BANK AND THIRD-PARTY PROVIDERS DISCLAIM ANY LIABILITY FOR ERRORS AND OMISSIONS CONTAINED IN THE CONTENT OF, OR DISPLAYED BY MEANS OF, THE WEBSITE. ALSO, THEY DO NOT WARRANT THE ACCURACY, COMPLETENESS OR ADEQUACY OF SUCH INFORMATION.

THE ONLINE BANKING, MX, BILL PAYMENT, EXTERNAL FUNDS TRANSFER, MOBILE BANKING, mRDC, TEXT BANKING SERVICES ARE PROVIDED TO YOU ON AN AS IS, AS

AVAILABLE BASIS. EXCEPT AS SET FORTH HEREIN, THE BANK AND THIRD-PARTY PROVIDERS DISCLAIM ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE, OR WARRANTY OF NON-INFRINGEMENT OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

THE BANK AND THIRD-PARTY PROVIDERS MAKE NO WARRANTY REGARDING LINKS TO THIRD-PARTY WEBSITES OR THIRD-PARTY PROVIDED SOFTWARE. USE OF OR ACCESS TO SUCH WEBSITES, THIRD-PARTY LINKS AND SOFTWARE IS DONE SO ENTIRELY AT YOUR OWN RISK.

G. Indemnification. You agree to indemnify, defend and hold us, our affiliate companies, directors, our officers, employees and agents harmless against any third-party claim, demand, loss, action, suit, or other proceeding, costs and expenses related to or arising from your use of OB, Bill Payment, MX, External Funds Transfer, Mobile Banking, mRDC, Text Banking, or other Services available now or hereafter.

H. Third Parties. We are not liable for any loss or liability resulting from any failure of your equipment or software, or the failure(s) of Q2 Software, Inc. (Q2), Fidelity National Information Services, Inc. (FIS Global), PNC Bank, N.A. (PNC Bank), MX Technologies, Inc. (MX), Ensenta Corporation (Ensenta), IDology, Inc. (IDology) or any of their processing agent(s), or those of any Internet browser provider, or any ISP. Nor will we be liable to you or any third-party for any direct, indirect, special or consequential damages resulting from your access/lack of access or use of the OB, MX, Bill Payment, External Funds Transfer, Mobile Banking, mRDC, Text Banking Services or your Accounts.

I. Virus Protection. The Bank is not responsible for any electronic virus or viruses malware or spyware that you may encounter through use of the Services. We recommend that you routinely scan your Computer or Mobile Device using a current virus protection product. An undetected virus may corrupt and destroy your programs, files, and your hardware.

XII. SYSTEM REQUIREMENTS; ACCESS TO SERVICES

System Requirements

To use OB, MX, Bill Payment, internal transfers, external funds transfer, Mobile Banking, mRDC, or Text Banking Services and to receive documents and information through Electronic Communications (ECs) you must have the following:

- Computer or Mobile Device with Internet access through an ISP
- Software providing access to portable document format (PDF) files, e.g. Adobe Acrobat Reader (available for free downloading at http://get.adobe.com/reader)
- Current valid email address
- Mobile Device, with messaging and data capabilities, for Mobile Banking
- Computer or Mobile Device, with scanner or camera function, respectively, for mRDC purposes

An Operating System and Internet web browser that:

- Supports 128-bit secure socket layer (SSL) encryption;
- Has cookies enabled; and
- Is Java Script enabled
- The OB platform supports most commercially accepted Operating Systems and browser versions. From time to time we may conduct system upgrades. Should any of them impair your ability to use the Services you will have the option of withdrawing.

Access to Services

To establish an Online account for OB purposes and to Enroll in and/or access Bill Payment, MX, External Funds Transfer, Mobile Banking, mRDC, or Text Banking Services you must affirmatively consent to receive information, data, disclosures (e.g. Account Disclosure Statements), records, notices and other communications in digital or electronic form, in accordance with the Electronic Signatures in Global and National Commerce Act, 15 U.S.C., Section 7001, et. al. (E-Sign Act).

Your consent must be given: (A) in a manner demonstrating your ability to access them in the way they will be provided, and (B) before you establish or use such Services.

You or an Authorized Person each demonstrate your affirmative consent during: (i) the Initial Log In process for OB, and/or Enrollment in (ii) the Bill Payment, (iii) MX, (iv) External Funds Transfer (v) Mobile Banking, (vi) mRDC, (vii) oe Text Banking Services.

You also consent when you or an Authorized Person: (A) use a temporary User ID and Password, and, when applicable, (B) complete the Bank's depositor identification procedures (including, for example, by answering questions and/or verifying micro-deposits and withdrawals), (C) create or use your own User ID(s), Password(s) or other Login Credentials, (D) request a Secure Access Code (SAC), (E) avail yourself of the security features of Enhanced Login, or (F) Log In to use the Services.

Legal Signature: Together, the User ID and Password will act as your legal signature, allowing access to the Services.

The Bank will provide instructions on how to use the Services. Ordinarily, you may gain access to your OB Accounts using a Computer or Mobile Device, your ISP, Password and User ID, 24 hours a day, seven (7) days a week. However, the Bank may suspend access for purposes of maintenance, updating and revising software, without liability to you.

The Bank's Business Days are Monday through Friday, beginning at 9:00 AM ET, excluding holidays and weekends.

XIII. YOUR ONLINE SECURITY

To access your Eligible Accounts or enroll in any of the Services, you will need a User ID and Password, which, when processed using multi-factor authentication (MFA) techniques and layered

security controls, will be used to validate your identity. We may establish or change the standards for a User ID, Password and other Login Credentials [Defined at Section XVII, herein].

When used with your User ID, your Password acts as an Electronic Signature and as your legal signature. You are solely responsible for keeping your User ID, Password and other Account and personal information (i.e. Login Credentials) strictly confidential.

Unauthorized Logins

Upon any Login to the Services by anyone using your User ID, Password, Login Credential or any other authentication control, the Bank may rely and act upon any instructions received under such circumstances. In the event of unauthorized use of your information, as described above, you will be liable for resulting losses, unless, following prompt notice of theft, loss or a possible breach of any of your Login Credentials, the Bank acts with gross negligence or willful misconduct in handling your request to block further use of the Services.

Although systems safeguards are in place, you, alone, are personally responsible for ensuring your own security Online. To help protect yourself against fraud and identity theft, you should follow these guidelines:

- Before every Log In on any Computer or Mobile Device verify the accuracy of your Last Log In date and time to ensure that you are accessing Apple Bank's website (and not some fraudulent site).
- When using a Mobile Device also exercise special caution and be on high alert to your surroundings, nearby persons and devices.
- Install and activate anti-virus, anti-spyware and anti-malware programs on your Computer or Mobile Device.
- Review and reconcile your Accounts on a regular, timely basis.
- Do not allow anyone to learn, access or view ANY of your bank, brokerage or other financial account data, information, statements or online capabilities, from ANY financial institution.
- Contact the Bank immediately if you receive unexpected correspondence from the Bank.
- Do not respond to email messages asking for personal or confidential information, even if they look like they came from the Bank. The Bank will not ask for such information via email messages. Any such message may be a Phishing attempt.
- Be on the alert to follow through if an expected welcome letter or other correspondence is not received.
- Do not share your User ID with others.
- Do not share your Password with others.
- Do not share your personal information, Login Credentials or Enhanced Login security questions or answers with others.
- Do not share your Account information with others.
- Do not walk away from a Computer or a Mobile Device when you are logged in to any service (e.g. OB, Bill Payment, external funds transfer, Mobile Banking, mRDC, Text Banking, , viewing account information, making inquiries or other OB Services, etc.
- Always exit and log off the system when finished.
- Change your Password periodically.

- Immediately change your Password if you have any reason to believe it has become known or available to others not authorized to access your Account(s) or Payment Account.
- Never leave your Account information, User ID or Password within range of others.
- Do not send confidential Account information (e.g. social security number or taxpayer identification number, account number, User ID, Password, security questions or answers, etc.) in any public, non-secure or general e-mail system.
- Review the terms and conditions of your agreement(s) with Q2, FIS Global, MX, Ensenta, , IDology and/or any subsidiary, affiliate or third-party processing agent (collectively, Third-Party Providers) to assure compliance with their procedures and/or requirements.
- Review the terms and conditions of all of Addenda to this Agreement for related Services to assure compliance with their procedures.

If you believe your Password or any other Login Credential has been lost or stolen, or if you suspect any fraudulent activity on your Account, call the Bank AT ONCE at (914) 902-APPLe (2775).Telephoning us is the best way to minimize your losses and liability.

Change your Password IMMEDIATELY if you have any reason to believe it has become known or available to persons without authority to access your Accounts or Payment Account.

Enhanced Login

Enhanced Login is a security feature that you enable by clicking Register Device, which deploys cookies to remember a specific Computer(s) and/or Mobile Device(s), recognizing their presence or absence when a Login is attempted. The process may also involve accessing detailed information including phone numbers, Computer and Mobile Device identification data and network identifiers.

Computers or Mobile Devices that are not registered will be identified and shall require an additional layer of security, i.e., through the delivery of Secured Access Code (see below). The Enhanced Login feature can improve your security and further protect you against potential fraud and identity theft.

The Bank recommends that, at a minimum, you regularly change your Password, and create a unique User ID and Password combination. Depending on the nature or magnitude of risk posed by one of more of the Services, the OB Services platform may employ additional MFA security techniques, including the use of challenge questions or Secure Access Codes (SACs) [Defined at Section XVII, see also, Access Security, below].

For protection against fraud and/or identity theft, the OB Services platform includes the following features relating to Access Security, Transaction Security and Transaction Limits.

Access Security

1. Secure Access Codes

   A secure access code (SAC) a randomly generated, one-time multi-factor authentication code delivered to a pre-populated and selected email address, phone or cell number (as a text message), i.e., the SAC target, which is valid for one-time use only and will expire if not used

promptly. The SAC is an enhanced security measure to further confirm your identity and authority to proceed, for examples, in the following situations:

At Initial Login;

- To register a Computer or Mobile Device;
- During subsequent Logins, if registration has not occurred;
- During transaction approvals, if transactions are of a certain type and amount that require extra authorization.

2. Multi-factor Authentication

Multi-factor authentication (MFA) is a layered security process by which:

(A) Things you know,
(B) Things you have, and/or
(C) Things you are

Must be furnished from independent sources of Login Credentials

Part of MFA involves a process called out-of-band authentication (OOBA), which is the delivery of a Login Credential in a channel other the one in which the User is banking and can involve verifying independently generated SACs.

MFA is for use in verifying a Users identity and authority to perform various transactions when using any of the Services and is used in the following situations:

- At Initial Login;
- During transaction approvals, if transactions are of a certain type and amount that require extra authorization [e.g., for Automated Clearing House (ACH) transactions; forgotten User ID or Password resets; wire transactions, etc.]

The MFA process may also include the use of an identity verification service, which access non-public financial information contained in consumer reporting agency and government databases that include non-public financial information and compare the information you provide with those authoritative sources. For those purposes Q2s third-party vendor is IDology, Inc. (IDology).

You hereby consent and authorize Q2 and IDology to access the User identity verification information received from such sources and to rely upon, compare and use it for MFA purposes and Know Your Customer and Customer Identification Programs under the Bank Secrecy Act (BSA), 31 U.S.C. 5311, et. seq. and its implementing regulations, in any circumstances involving the use of the Services including but not limited to the following functions:

- Enrollment in OB and any of the Services hereunder
- At Initial Login
- When establishing/modifying a SAC target
- During subsequent Logins, if registration has not occurred
- When a User ID or Password is forgotten
- During transaction approvals, if transactions are of a certain type and amount that require extra authorization
- As part of Risk and Fraud Analytics (RFA); see sub-section 6., below

3. Session Expiration Timers

For added security, Apple Bank's Mobile Banking application does not allow Users to save their User IDs and Passwords. In addition, session inactivity and session life timeouts are employed. For general OB security precautions, please see Your Online Security, below.

4. User Management Definitions

The Bank sets Group Level categories for assigning the first layer of rights and limits for Users. At the Customer Level, there are two classifications, Household or Commercial, and beneath that tier level there are Users. Rights and limits are passed down from the Group Level. User permissions and authority for OB Services, within those tiers, are prescribed, granted and set in accordance with these Management definitions and may be limited. Dual approval controls are available (e.g., for Commercial customers).

Transaction Security

5. MFA See above, at 1.

6. Risk and Fraud Analytics (RFA)

In addition to MFA, risk and fraud analytics (RFA) are employed to detect and protect Users from potential fraud, for example, by monitoring suspicious characteristics of requested External Funds Transfer(s), possibly placing them on hold and providing an opportunity to verify the authenticity of the transaction.

As noted above at sub-section 2. MFA processes are also applied as a result of RFA and IDology may access third-party information sources to help identify the User.

7. Security Alerts; Optional Alerts

There are two kinds of alerts that will be sent to your chosen SAC Target. The first type is a Security Alert, which related to suspicious or potentially fraudulent activity that could affect you or your Account. These may arise from the RFA process described immediately above.

The second type of alert is an optional alert, which the User chooses to set up so that specific Account information might be sent to the Users SAC target.

Transaction Security (Limits)

8. Group Settings For the selected Group Level, the Bank assigns the parameters of the rights or permissions that are available to customers and the associated limits within them. For example, the transaction rights or permissions may include various component parts of the Services (e.g., Bill Payment, External Funds Transfer, Mobile Banking, mRDC, Text Banking, etc.). While the associated aggregate limits on those rights could pertain to numbers or dollar amounts, per day, per transaction, per month, etc. The types of Security Alerts available to Users can also be set at the Group level.

9. Customer Rights Within the Group Level, the Bank reserves the right to limit Customer Level Rights and permissions, as well as limits therein, relative to the available OB Services.

10. User Rights Individual limits can be set at the User Level, for example, in the Commercial context.

XIV. ELECTRONIC COMMUNICATIONS AND YOUR RIGHTS

Types of Electronic Communications

Documents and information delivered through electronic communications (ECs) may include of consumer disclosures required under law, including Account Disclosure Statements, such as initial and subsequent disclosures, periodic statements, annual statements, records, notices (e.g. notices of changes in terms, renewal notices, etc.), e-mail messaging, Text Banking, related information and other communications. Upon your consent to this Agreement, the Bank reserves the right to deliver all written communications to you through ECs. By way of example, but without limitation, these communications could include:

- OB Service Agreement (the Agreement)
- Any Addenda thereto (e.g., for external funds transfer, Mobile Banking, mRDC, Text Banking, etc.)
- About Your Apple Bank Accounts
- Schedules of Maintenance and Service Charges
- Initial Account Disclosures for certain deposit account products
- Initial Account Disclosures for certain credit account products (e.g. personal loans, overdraft lines of credit, secured loans, secured lines of credit, security agreements, etc.)
- Service information
- Notices of changes to any of our agreements, addenda, terms, conditions, policies or Account disclosures
- Text Banking, messaging and account information
- Secure Access Codes (SACs)
- Periodic and other statements of Account balances, transfers, transactions, activity and other information relating to Eligible Accounts, including, but not limited to, periodic e-Statements
- Subsequent Account Disclosures (e.g. changes in account terms; renewals)

- Apple Bank for Savings and Affiliates' Annual Privacy Policy Notices
- Opt-In or Opt-Out Notices and Forms
- Bill Payment Service account information
- External Funds Transfer information
- Confirmations of account transactions or activity
- Inquiries or notices about transactions made using OB, Bill Payment, MX, external funds transfer, Mobile Banking, mRDC, Text Banking, etc.
- Security Alerts and notifications (e.g. of possible unauthorized account access, data intrusions, etc.).
- Notices of Password changes
- Notices of User ID changes
- Notices of other changes (e.g., Login Credentials, etc.)
- Notices of email address changes (sent to both new and old addresses).
- Notices of newly added Bill Payment Payees.
- Information about Enhancements to the Services.
- Information about balance transfers between Eligible Accounts that you initiate through OB.
- Information about payments of minimum or other outstanding loan balance amounts
    - (A) by transfers between Eligible Accounts, or
    - (B) by payments you initiate through your Bill Payment Account.
- Inquiries or notices to you concerning the resolution of any claimed error on your periodic statements
- Information concerning Account fees and charges
- Information about stop-payment orders you initiate through the OB, Bill Payment or External Funds Transfer Services Safe deposit box contracts, renewals, changes and related information
- Any other information or notices concerning your Account(s), EFTs or transactions

Your Rights Regarding ECs

Regarding your consent to receive ECs from Apple Bank, you have the following rights:

Scope. Your consent to receive ECs applies to all Eligible Accounts and Services accessible by you through the OB, Bill Payment, MX, internal transfers, external funds transfer, Mobile Banking, mRDC, or Text BankingServices.

Bill Payment or Activity. If you Enroll in Bill Payment or External Funds Transfer (External Funds Transfer Agreement), your activity using such Services will be reflected on your periodic statements.

Withdrawal. You may withdraw your consent to receive ECs by notifying the Bank in writing at:

Digital Banking Services
c/o Apple Bank for Savings
900 Stewart Ave
Suite 605
Garden City NY 11530

Consequences of Withdrawal. The Bank will not assess a fee if your withdrawal is due to a material change in the Bank's System or Software requirements. Following withdrawal of your consent you will not be able to access the Services. Withdrawal could result in (A) cancellation or non-payment of one or more scheduled Bill Payments, External Funds Transfer, mRDC, or Text Banking Services, and (B) the imposition of third-party fees.

Contact Information. Whenever you change your email address or other contact information you must promptly update your information with the Bank so we can continue to communicate with you in a timely manner. Updating such information can be done securely through OB Service, following the instructions and prompts, under Settings and, then, Profile.

Need for Paper Copies. You may obtain paper copies of documents you access through the Services. You may:

(A) print them from the Computer screen or Mobile Device when establishing or using the Services,
(B) go to www.applebank.com, locate and print the document,
(C) send a written request to CustomerLine (as set forth above, under Withdrawal) identifying the necessary records, or
(D) come to any branch and request a paper copy.

XV. ENHANCEMENTS TO SERVICES

The Bank may add new or modify Services, their functionality, features or the capabilities of OB, Bill Payment, internal transfers, External Funds Transfer, Mobile Banking, mRDC, and Text BankingServices (Enhancements). If we do, you will be apprised of material changes in terms and conditions. Thereafter, if you do not terminate the agreement(s) and continue to use the affected Service(s) you will be deemed to have confirmed your acceptance of those terms and conditions. All other terms and conditions of this Agreement and Rules, as amended, will continue to apply.

XVI. GENERAL TERMS AND CONDITIONS

A. Bank and Other Agreements. You agree to be bound by this Agreement and to comply with all other agreements, rules, regulations, policies and practices applicable to your Online Account, your Accounts, products and services, including but not limited to agreements with the following Third-Party Providers:

(1) Q2 Software, Inc. (Q2),
(2) FIS Global, for Bill Payment Services,
(3) The originating depository financial institution (ODFI) for External Funds Transfers, or
(4) MX Technologies Inc. (MX),
(5) Ensenta Corporation (Ensenta), for mobile remote deposit capture,
(6) IDology, Inc. (IDology) for customer identity authentication and verification, and
(7) Any of their subsidiaries, affiliates or third-party processing agent(s) for the respective Services.

The terms, conditions and privacy policies that relate to the services of Q2, FIS Global, PNC Bank, MX, Ensenta, , IDology and any of their processing agent(s), as applicable, shall also

apply to your non-public personal information in connection with the Services performed when communicating with their web servers in those regards.

B. Electronic Signature: Your Initial and subsequent Logins and, when applicable, your Enrollment and sign-on in any of the Services each shall constitute your Electronic Signature and will be binding upon you, your heirs and successors, as your legal signature. Similarly, each use by you or your Authorized User of your User ID and Password shall also constitute your binding legal signature.

By using OB or any of the Services you acknowledge receipt of the agreements described above, together with all related disclosures, and intend to be bound by them. You should review all Account Disclosure Statements and disclosures, charges that may apply for making EFTs and the fee schedule contained in this Agreement. Each month, if applicable, we will automatically deduct fees related to Bill Payment or External Funds Transfer Services from your Payment Account.

C. Changes and Modifications. The Bank may modify the terms and conditions applicable to the Services from time to time. We may send any notice to you via e-mail and you will have to be deemed to have received it three (3) days after it is sent. The revised terms and conditions shall be effective at the earliest date allowed by applicable law.

D. Termination Without Cause. We reserve the right to terminate this Agreement and your use of the Services in whole or in part at any time without prior notice.

E. Assignment. We may assign this Agreement to an affiliate of the Bank or any successor in interest in the event of a merger, reorganization, change of control, acquisition or sale of all or substantially all assets of the business to which this Agreement is related without the other party's prior written consent.

F. Notices. Unless otherwise required by applicable law, any disclosures, notices or written communications to be given pursuant to this Agreement may be sent to you electronically (i.e. through ECs).

G. Disclosure of Information. We will only disclose information to third parties about your Accounts, accounts at other FIs and EFT transfers that you make under the following circumstances:

- When necessary to perform or complete requested other transactions and for the provision, generally, of OB, MX Services, Bill Payments, External Funds Transfer, Mobile Banking, mRDC, and/or Text Banking Services.
- When necessary to resolve claimed errors or other questions involving your Online Account, your Payment Account, Eligible Accounts or any of the Services, as mentioned above.
- To verify the existence and condition of your Account for a third party, such as a credit bureau or a merchant.
- To comply with government or court orders, legal process (e.g. subpoena) or other reporting requirements.

- If you give us or the person asking for information your permission.
- To Bank affiliated companies, as permitted under the Bank's Privacy Policy.

H. Disclosure of Information to Q2, MX, FIS Global, PNC Bank, Ensenta, IDology, Inc. and/or any processing agent(s). If you apply for or use OB, MX, Bill Payment, External Funds Transfer, mRDC, or Text Banking Services, you are subject to the separate Privacy policies, of Q2, MX, FIS Global, PNC Bank, Ensenta Corporation (Ensenta, IDology, Inc. (IDology) and/or any of their subsidiaries, affiliates or processing agent(s). Such policies should be carefully reviewed before you transmit any non-public personal information during the Account application and customer identification process.

I. Governing Law, Jurisdiction and Venue. The laws of the State of New York law shall govern this agreement, any Addenda thereto and the Account relationships created and the Services furnished thereunder, without regard to conflicts of law provisions thereof.

By creating a User ID and Password, and/or by maintaining an Account that may be accessed hereunder through ECs, you agree that: (1) either the United States District Court for the Southern District of New York or the Courts of the State of New York shall have exclusive jurisdiction over you and the Account, and (2) that proper venue for any action arising out of that relationship, respectively, shall be either in the Southern District of New York or in New York County. The depositor waives any objections to such jurisdiction or venue.

J. Severability. If any one or more terms, conditions or provisions of this Agreement or any of the Addenda thereto is found to be invalid or unenforceable, that provision will be enforced to the maximum extent permissible, and the remaining provisions will remain in full force.

XVII. DEFINITIONS

The following definitions apply:

1. External Funds Transfer Service is a service offered by the Bank pursuant to a supplemental agreement enabled upon Enrollment, through which you can initiate certain external funds transfers through ACH to or from one or more of your External Accounts, with certain limitations (see External Funds Transfer Agreement).

2. Account includes a deposit, credit or loan account maintained with Apple Bank and designated for access to OB Services.

3. Account Disclosure Statements include any document(s) setting forth broad Account terms and conditions, fees and charges, as well as individual disclosures for or notices relating to your Accounts. They could pertain to personal or business Accounts and, when applicable, include loan notes, line of credit and security agreements.

4. Apple Bank's Business Address is: Apple Bank for Savings, 122 East 42nd Street, New York, NY 10018.

5. Apple Bank's CustomerLine Service Phone Number is (914) 902-APPLe (2775).

6. Apple Bank Website is the site located at the following Uniform Resource Locater (URL): http:/www.applebank.com.

7. "Authorized Person" refers to any person or Entity to whom you have given authority to access one or more OB and other related Services available thereunder, individually or acting in any other authorized legal capacity.

8. Automated Clearing House or ACH refers to the electronic payments system through which you may:

(A) initiate debits against or credits to your External Account(s) using external funds transfer, for purposes of making withdrawals from and deposits to your external Account(s),
(B) make Bill Payments from your Payment Account

9. Bill Payment Service is the Service available for making or scheduling Bill Payments and may include e-Billing services.

10. Business Day is any day other than a Saturday, Sunday or legal bank holiday.

11. Computer is a personal computer or a mobile device, smart phone, personal digital assistant or other hand held device capable of accessing the Internet (Mobile Device) via dial-up, cable modem, wireless access protocol, or equivalent, supports the System Requirements set forth herein, and which, when using an adequate Internet browser and your ISP, enables you to access your Online Account and, upon Enrollment, Bill Payment, MX, external funds transfer, Mobile Banking, mRDC, Text Banking, or other Services.

12. Deliver By Date means the date by which you can expect the Bill Payment to be received by the Payee. It is the date associated with and follows the Send On Date that you select when scheduling a payment(s), on a recurring or nonrecurring basis. To ensure timely processing, you should make your selection(s) not later than two (2) Business Days before the actual due date reflected on your payee statement. If the actual due date falls on a non-business day, you should select a Deliver By Date that is at least one (1) Business Day before the actual due date on the payee statement.

13. EC or Electronic Communication means an electronic delivery or exchange of information or messages that can be read as visual text and displayed on a Computer or Mobile Device occurring between you and the Bank. We may deliver any EC to you: (1) directly on a Computer screen or Mobile Device or (2) through web links (including non-by-passable web links), (3) email or text messaging, or (4) posting on the Apple Bank Website.

14. Electronic Funds Transfers (EFTs) include, but are not limited to, funds transfer transactions, including external funds transfer, based on your authorization and direction depending on which Service is being accessed to the Bank, Q2, Fidelity National Information Services, Inc. (FIS Global), for forwarding to an ACH Network and/or any of their subsidiaries, affiliates or third-party processing Agent(s) to electronically:

(A) Transfer funds through debits or credits to or from your Eligible Accounts,
(B) Direct and initiate payments through your Bill Payment Account,

(C) Make Withdrawal Instructions (defined herein), or
(D) Make ACH transfers through the external funds transfer Service (see External Funds Transfer Addendum to this Agreement) between your External and Eligible Account(s).

EFTs are defined under the Electronic Funds Transfer Act, 15 U.S.C. Section 1693 et. seq. (Act) and Federal Reserve Board Regulation E, 12 C.F.R. Part 1005, and Official Staff Interpretations at Supplement I (Reg. E).

15. Electronic Signature is an EC made and delivered by you (or with your authority) indicating your consent to this Agreement. Each use and submission of your User ID and Password:

(1) acts as your legal signature,
(2) qualifies as an electronic signature under 15 U.S.C. 7006(5), and
(3) signifies your continued acceptance of
(a) this Agreement and, if applicable,
(b) your agreement(s) with any of the Third-Party Providers of Services referenced in this Agreement and any Addenda thereto.

16. Eligible Account(s) means any credit, loan, line of credit, statement savings, checking, negotiable order of withdrawal (NOW), certificate of deposit (CD) or money market (MMA) account maintained with the Bank that are accessible for Services, as determined by the Bank. Access for certain OB (e.g. making EFTs) and Bill Payment Services may be prohibited in some cases.

Ineligible accounts include those held in certain fiduciary capacities (e.g. by estate representatives, non-grantor trustees, guardians, etc.), subject to court order or activity restrictions (e.g. passbook accounts), Youth accounts, etc. You may not make EFTs to or from a credit card, co-operative loan or mortgage account.

17. Enhanced Login is a security feature enabling you to Register your Computer(s) or Mobile Device(s) after verifying the Secure Access Code (SAC) furnished during your Initial Login. The process uses cookies and other identifying information, so that you will not need to repeat the SAC verification process each time you login. For security purposes, non-registered Computers and Devices will require further information to verify the Users identity and authority to proceed.

18. Enrollment is the process through which you electronically enroll (or as otherwise permitted) in OB, Bill Payment, MX, external funds transfer, Mobile Banking, mobile remote deposit capture (mRDC), Text Banking, or other Services hereunder, the terms and conditions of which are described herein, in separate Enrollments, Addenda hereto and in your agreements, respectively, with Q2, FIS Global and PNC Bank, Ensenta, or IDology. You Enroll by clicking: (1) I Accept at the end of each presented set of Terms & Conditions, signifying your assent, and (2) SUBMIT at the close of the registration page(s).

19. External Account is a transactional (i.e. checking or savings) account that, ordinarily, you maintain with a third-party U.S. FI (or sometimes with us) and designate to associate and link with one or more of your Eligible Accounts, electronically via ACH, subject to transactions limitations (see External Funds Transfer Agreement; see also, Section I. C, above, External Funds Transfer Service)

20. Initial Log In. When you use a Computer or Mobile Device to access OB or the Services, create a User ID, use a Password and click on the I Accept button, you are representing that you: (A) have read, understand and agree to the Agreements terms and conditions, and (B) consent to receive ECs from the Bank. You are also signifying your consent to participate in OB and related Services, and, upon Enrollment, your further promise to abide by Q2s terms and conditions.

21. "ISP" refers to your Internet Service Provider.

22. Login Credentials may include, but are not limited to, User IDs, Passwords, email address(es), phone number(s), security questions and answers, Secure Access Codes, one-time passwords, device identifiers, etc.

23. "OB" is the Bank's internet-based service providing access to your Eligible Account(s) including, if applicable, your Bill Payment and External Funds Transfers, via Computer, Mobile Device, Operating System(s), Web Browser(s), User ID and Password.

24. "Online Account" means any Eligible Account from which you may view or conduct transactions using a Service.

25. "Password" is the personal code you create and select for use during OB Log In and includes any code you create or select thereafter which, when used with your User ID, permits access to one or more of the Services. Each such Password supersedes those previously created by the Bank (for temporary use) or by you.

26. Payment Account is the checking account from which Bill Payments will be debited.

27. Payment Instruction is the information you furnish through ECs to FIS Global to enable a Bill Payment to be scheduled, including the amount, payee name, payee account number, the Send On Date, and, when applicable, the associated Deliver By Date.
28. Properly Scheduled Payment is one made from your Payment Account with sufficient available funds for the payment and associated fees scheduled to be delivered on or before the due date of the bill, excluding grace periods, indicated to be deliverable on time and for which the information supplied is correct and is not a prohibited payment under the Service.

29. Secure Access Code or SAC is a randomly generated one-time multi-factor authentication code delivered to a pre-populated and selected email address, phone or cell number (as a text message), that is used as an enhanced security measure to further confirm your identity as the true User or Authorized Person during Login and/or when using a Computer or Mobile Device.30. Send On Date is the date when the processing of any Payment Instruction begins (at sessions end) and, in the case of electronic debits, is also the date on which your Payment Account will be debited for the scheduled Bill Payment.
31. Services, as applicable hereunder or any Addenda hereto, may include OB, MX, Bill Payment, internal transfers, external funds transfers, Mobile Banking, mobile remote deposit capture (mRDC), Text Banking, and other Services available to Users now or hereafter.

32. Third-Party Providers include:

a) Q2 Software, Inc. (Q2)
b) FIS Global, for Bill Payment Services
c) The originating depository financial institution (ODFI) for External Funds Transfer, or
d) MX Technologies Inc. (MX)
e) Ensenta Corporation (Ensenta), for mobile remote deposit capture
f)
g) IDology, Inc. (IDology) for customer identity authentication and verification, and
h) Any of their subsidiaries, affiliates or third-party processing agent(s) for the respective Services.

33. "Time of day" references are to Eastern Time (ET).

34. User ID, depending on context, is either a Bank generated or customer created identification code assigned to or created by you that, when coupled with your Password, will allow access to OB and, upon Enrollment, MX, Bill Payment, internal transfers, external funds transfers, Mobile Banking, mRDC, Text Banking, other related Services.

35. "We", "us", Apple Bank or "Bank" refer to Apple Bank for Savings which offers the Services and which holds the Accounts accessed through the Services.

36. "You" or "your" refers, as applicable, to those persons or entities (including any Authorized Persons) that (A) apply to use and/or use any of the Services, and (B) own or control an Account.