SOLVAY BANK

Business Electronic Services Guide to Services

CUSTOMER SUPPORT

General Customer Service

Support for: Balance and account information, Bill Pay, Transfers and User set up

Contact Information

- Phone – 315-484-2201
- E-Mail – customercare@solvaybank.com

Service Hours

- Monday – Wednesday: 8:00 AM – 5:00 PM
- Thursday – Friday: 8:00 AM – 6:00 PM
- Saturday: 9:00 AM – 12:00 PM

Advance Support for Cash Management Services

Support for: Problems processing ACH, Wires, Positive Pay or iBank.

Contact Information

- Jeanette Armstrong, Cash Management Ops Specialist
  E-Mail – jarmstrong@solvaybank.com
- Dawn Brown, Card & Payment Specialist
  E-Mail – dbrown@solvaybank.com

Service Hours

- Available Monday-Friday 8:30 AM to 4:30 PM

Please contact your relationship manager if you would like to add an additional service to your account. They can provide you general service information and applicable fees for services.

SERVICE AVAILABILITY & CUT-OFF TIMES

Business Electronic Services are available 24-hours a day. End of day cut-off times for each applicable service are listed below.

ACH File Cut-Off Time:

- Next Day ACH: 2:00 PM EST

Wire Transfer Cut-Off Time:

- Domestic Wire Transfers: 2:30 PM EST
- International Wire Transfers: 2:30 PM EST

iBank Remote Deposit Cut-Off Time:

- Daily Deposit: 4:00 PM EST

Positive Pay Exception Review Cut-Off Time:

- Exception review time frame: 8:00 AM – 11:00 AM EST

Standard Business Day Cut-Off Time:

- Same Day Business – items initiated before: 5:00 PM EST
- Next Day Business – items initiated after: 5:00 PM EST

To avoid overdrafts or exceed available credit limits, Bank recommends all Company Representatives, who may access accounts to perform any transfers, payments, debits or advances be made aware of these cut-off times.

BUSINESS DAY HOURS & BANK OBSERVED HOLIDAYS

A business day is defined as a legal banking day where Solvay Bank is open for business, such as every day except Saturdays, Sundays and holidays as noted below. In general, the Bank business day hours are from 8:00 AM EST to 5:00 PM EST. Please visit our website for specific branch location availability.

Bank Observed Holidays:

New Year's Day	January 1	Labor Day	First Monday in September
Martin Luther King Jr. Day	Third Monday in January	Columbus Day	Second Monday in October
President's Day	Third Monday in February	Veteran's Day	November 11
Memorial Day	Last Monday in May	Thanksgiving Day	Fourth Thursday in November
Independence Day	July 4	Christmas Day	December 25

When the holiday falls on a Saturday, it is usually observed on the preceding Friday. When the holiday falls on a Sunday, it is usually observed on the following Monday.

BANK CONTACT INFORMATION

Notices to Bank may be delivered:

Via US Mail
Solvay Bank
PO Box 19050
Syracuse NY 13209

In person or via delivery agent
Solvay Bank
1537 Milton Avenue
Solvay NY 13209

EDUCATIONAL INFORMATION

Educational information including video tutorials and service Quick Reference Guides may be found by visiting our website https://www.solvaybank.com/education.

BUSINESS ONLINE BANKING

IDs/Passwords

- User ID and User Password are required to sign in.
- The IDs must be 4-16 characters in length (numbers, letters or these symbols: !, @, #, $, &).
- The Passwords are case-sensitive and must be 8-17 characters in length, contain 2 or more alphabetic characters, contain 1 or more uppercase alphabetic characters, contain 1 or more lowercase alphabetic characters, 1 or more numeric characters and 1 or more special characters and must NOT contain any spaces.
- The User Password expires every 180 days.

User Definitions

- Senior Administrator – The person who is the primary user and main Business Online Banking contact for the Company. There can be only one. Has access to all services for which the company has signed up. They can create payments, manage online billing and payments, review transfers, assign administrators, complete administrative functions online, modify permissions and establish all users with all security levels.
- Administrator – Assigned by the Senior Administrator, can approve expenditures, set up users and they can create payments, manage online billing and payments.
- User – End user set up on the system by Senior Administrator or Administrator. Has limited authority to manage payment accounts, online billing, and payments with dual control.

Initial Password Set-Up

The Bank will set Company ID, User ID and the initial Company and User passwords for the Senior Administrator. The Senior Administrator is prompted to change both passwords upon first log-in. The Senior Administrator must set up any other Administrator(s) and or User(s) and their initial passwords, which must be updated upon their first log-in.

Password Changes

All end-users can change their own User Password. Only the Senior Administrator or Bank can change the Company Password.

Lockout

After three consecutive, unsuccessful attempts to log into the system, the user will be locked. This failed login count is incremented by a Multi-Factor Authentication challenge, as well. With each successful login, the failed login count is reset to zero.

Forgotten Passwords/Lock Outs

- The Senior Administrator must be unlocked and/or have their password reset by the Bank. The Bank has access to unlock/reset the Senior Administrator only.
- Administrators must be unlocked and/or have their password reset by the Senior Administrator.
- Users must be unlocked and/or have their password reset by the Senior Administrator or Administrator.

Inactivity Time-out Feature

Although it is recommended that customers, or end users, never leave their computers unattended while logged into Business Electronic Services; a built-in security feature minimizes the risk in such a situation. The inactivity time-out feature ensures that Business Electronic Services automatically shuts off after a designated period of inactivity. The Senior Administrator can specify the length of inactivity before Business Electronic Services shuts off. If no time is set, a default time of 10 minutes is automatically used.

Enhanced Multi-Factor Authentication (MFA)

This security feature provides a two-factor authentication to access Business Electronic Services. After valid login credentials are entered, if the system does Not recognize the computer, it will challenge the user to answer a security question. After answering the question correctly, the end user has the option to register their computer, and a browser-based secure cookie will be stored on the user's computer which will recognize the user in for future visits. This cookie will employ a complex device identification process using the browser, the browser version and IP address as part of the identifying criteria.

These are some of the conditions that could trigger the end-user to require a new one-time passcode after enrollment:

- The IP address is different
- The browser or browser version is different
- The location is different
- The cookie has been deleted from the browser

AUTOMATED CLEARING HOUSE (ACH) ORIGINATION

ACH Rules

All ACH input files must be in the standard ACH format based on the NACHA Operating Rules. NACHA Rules may be obtained at NACHA's website at www.NACHA.org or by contacting NACHA directly at 703-561-1100. Files must be balanced and contain offsetting debit and credit entry totals. Files over a company's Limit may require approval or not be sent.

Types of Entries

ACH Type Codes are payment types used by Originators to identify whether debit or credit entries are being transmitted. Each ACH Type is recognized by a specific Standard Entry Class (SEC) code which also identifies the specific record layout that will be used to carry the payment. Company may use Business Electronic Services, to originate, create, and/or deliver PPD or CCD/CTX NACHA formatted files for further processing.

- Cash Concentration or Disbursement (CCD): Either a credit or debit where funds are either distributed or consolidated between corporate entities. May have one addenda record attached (CCD+)
- Corporate Trade Exchange (CTX): The transfer of funds (debit or credit) within a trading partner relationship in which payments related information is placed in multiple addenda records. (up to 9,999 addenda records).
- Prearranged Payment and Deposit Entry (PPD): Direct Deposit and Direct Payment
- Direct Deposit - The transfer of funds into a consumer's account. Funds being deposited can represent a variety of products, such as payroll, interest, pension, dividends, etc.
- Direct Payment - Preauthorized payment is a debit application. This includes recurring bills that do not vary in amount -- insurance premiums, mortgage payments, charitable contributions, and installment loan payments or standing authorizations where the amount does vary, such as utility payments.
- Tax Payments: Enrollment Requirements and Special Requirements of Federal tax payments. The Company warrants that it has enrolled in the Electronic Federal Tax Payment System (EFTPS) and has selected the ACH credit option. The Company warrants that all special requirements of the EFTPS system will be met, including the generation of prenotification entries before the first tax payment is sent. The Company further warrants that it is generating the tax payment, it will use the CCD format with a TXP Addenda record as required.

Transmission Methods

1. PC/Internet Transmissions through Business Electronic Services System. File transmission using Business Online Banking and related Services requires a valid Access ID and password.
    - The Company's authorized representative will access the System by utilizing the prearranged log-on procedures and additional verification processes, included but not limited to, use of security questions and answers, internet browser "cookies", and one-time password devices (e.g. tokens).
    - The Company's authorized representative will provide Bank with verification of the totals contained in the transmission. The system will verify that the file totals agree with the file provided. In the event of a discrepancy in the totals, the system will not accept the file.
2. PC/Internet Transmissions through our secure mail server. This option is only available as a back-up option when Business Electronic Services are not working and the system is not able to accept or process files. You may contact our General Customer Service line to initiate this process.
    - The Company's Authorized Representative will contact Bank to initiate secure mail process to send file. Each file must be accompanied by a transmittal register signed by an authorized signatory (representative) as set forth on the Business Electronic Services Resolution.
3. Hand delivered files or files by Courier. Files may be delivered to the following location as a last effort if both option 1 & 2 are not available. Delivery must occur prior to the cut-off time listed to be processed the same day. You may contact our General Customer Service line to give advance-notice of delivery to the following address:

    Business Electronic Services, Solvay Bank, 1537 Milton Avenue, Solvay, NY 13209

    - The Company's Authorized Representative will contact Bank to give advance-notice of file delivery. Each file must be accompanied by a transmittal register signed by an authorized signatory as set forth on the Business Electronic Services Resolution.

Electronic File Transmission

Solvay Bank will anticipate the receipt of an ACH file transmission from Company on each scheduled processing date identified by Company in writing and agreed to by Solvay Bank. Company is responsible for ensuring that Solvay Bank receives the transmission on each processing date indicated in the processing schedule. Company's Authorized Representative(s) will notify Solvay Bank if a transmission will not take place on the prearranged scheduled processing date.

Solvay Bank will verify that the file totals agree with Company information given. In the event of a discrepancy in the totals, Solvay Bank will call the specified Company Authorized Representative(s) designated by an authorized signatory of Company. If the Authorized Representative(s) are not available for notification, the file will not be processed until Company's Authorized Representative(s) can be contacted on the next business day.

Company is solely responsible for the accurate creation, modification, and deletion of the account information maintained on the Company's personal computer and used for ACH money transfer. Company agrees to comply with written procedures provided by Solvay Bank for the creation, maintenance, and initiation of ACH money transfers. Company is solely responsible for access by its employees of the data files maintained on Company's computer and for operator security procedures on the personal computer licensed for use of the program.

- Same-Day ACH Processing Schedule
    - A morning submission deadline at 10:30 AM ET, with settlement occurring at 1:00 PM
    - An afternoon submission deadline at 2:45 PM ET, with settlement occurring at 5:00 PM

  (These are the NACHA established deadlines. Each Financial Institution will set their own cut-off times for Same-Day ACH.)

- Same-Day ACH Credit

  Beginning September 15, 2017, Same-Day ACH will be available for debit entries, enabling the same-day processing of virtually any ACH payment. RDFIs will be mandated to make funds available from Same-Day ACH credits (such as payroll Direct Deposits) to their depositors by 5:00 PM at the RDFI's local time.

- Same-Day ACH Debit

  Beginning March 16, 2018, RDFIs will be mandated to make funds available from same day ACH credits (such as payroll Direct Deposits) to their depositors by 5:00 PM at the RDFI's local time.

IBANK REMOTE DEPOSIT SERVICE

Check Retention and Destruction

Solvay Bank's policy requires the check writer's check to be securely stored for 45 days after processing, then destroyed. Check images are retained by the processor for research and to comply with regulatory requirements. In the event of a deposit dispute Solvay Bank may require presentation of the original check to settle the dispute.

System Requirements for Workstation Hardware & Software:

Hardware

2.0GHz (or higher) processor recommended

2 GB of RAM (or higher) recommended (1 GB minimum)

Check Scanner (see list of approved scanners)

Disk Space

11 to 20 GB of available disk space on the system drive recommended

Operating System

Mac OS X 10.11 (Certified)

Microsoft Windows 7 - 32-bit (Supported)

Microsoft Windows 7 - 64 bit (Certified)

Microsoft Windows 8.1 - 64 bit (Supported)

Microsoft Windows 10 - 64-bit (Supported)

Software

Microsoft .NET Framework Version 2.0 with Service Pack 1

Appropriate Ranger Device Driver

Browser

Apple Safari 8.0 (Supported)

Apple Safari 9.0 (Supported)

Apple Safari 10.0 (Supported)

Microsoft Edge for Microsoft Windows 10 (Certified)

Microsoft Internet Explorer 11.0 (Supported)

Other

High-speed Internet connection is required (e.g., Cable, FiOS, DSL, T1)

Scanner Types:

Scanners can be obtained through any scanner vendor of the company's choosing. Solvay Bank can also refer the customer to a scanner vendor if preferred. These are our current vendors for purchasing scanning equipment:

Company: ComSRS Systems Inc.

Company Website: www.srssystem.com

Contact: Richard E. Lamb, Jr.

Contact Phone: 315-458-7813 or 800-875-6565

Contact Email: rlamb@srssystem.com

Company: UniLink

Company Website: www.unilinkinc.com

Contact: Matt Diehl

Contact Phone: 585-248-2980 or 800-666-2980 ext 16

Device Certification Status Definitions

- Certified — All functions of the product have been through certification testing.
- Supported — Basic functional testing of the product has been performed and has not revealed any major issues. It is recommended that individual company testing occur prior to use with iBank processing.
- Not Supported — Testing of the product is not planned. It is not recommended that individual company use for iBank processing.

Certified Scanners

- Burroughs Merchant Elite
- Burroughs Micro Elite
- Burroughs Professional Elite
- Burroughs SmartSource Edge
- Burroughs SmartSource Micro Elite SE
- Burroughs SmartSource Professional
- Canon CR-50
- Canon CR-80
- Canon CR-135I
- Canon CR-190I
- CTS LS100 (Microsoft Windows only)
- CTS LS150 (Microsoft Windows only)
- Cummins Allison JetScan iFX i100 (Microsoft Windows only)
- Digital Check CX30
- Digital Check TS215
- Digital Check TS240
- Epson TM-S2000 (Microsoft Windows only)
- Panini i:Deal
- Panini Vision 1
- Panini Vision neXt
- Panini VisionX
- Supported
- Canon CR-25
- Canon CR-55
- Epson Capture One (TM S1000)

Supported Scanners

- Canon CR-25
- Canon CR-55
- Epson Capture One (TM S1000)

Not Supported Scanners

- Burroughs SmartSource Adaptive
- Burroughs SmartSource Micro Series
- Burroughs SmartSource MicroEX
- Canon CR-180
- Canon CR-180II
- Digital Check TS230
- MagTekExcella
- RDM EC7000i Series

Scanner Drivers:

The scanner you purchase will not come with the appropriate iBank drivers. You can obtain these drivers inside Business Online Banking.

FAQ - Frequently Asked Questions:

- What happens if a check cannot be deposited through iBank?
  You may bring the item to the Bank for deposit or mail in the item with a deposit slip. This may occasionally happen due to poorly printed checks.
- Once a check has been presented, can it be stopped?
  Once the check has been scanned, prior to the procession of the check at the system cut off time, your system administrator or certain users may have the right to edit or cancel a pending deposited item. After the cut off time the transmission cannot be stopped.
- What happens if I receive cash?
  Unfortunately, you are not able to deposit cash with your scanner. All cash must be deposited at the bank.
- How would I be notified of a return?
  You will be notified by the bank regarding any returns. The bank will provide an image replacement document (IRD).
- May items be presented again?
  Contact the bank for special instructions for IRDs returned.
- How do I correct a mistake, for example, when the item is scanned twice?
  If the batch has not been processed, your administrator or certain users can still edit the deposit and correct your mistake or remove the item completely. If the deposit has been processed, you must contact Solvay Bank immediately so the Bank can attempt to intervene. There is a safeguard built into the software to flag duplicate checks that have recently been scanned.
- Will I have access to the check images to review items I have deposited using iBank?
  Yes, you will be able to access the images through the report module when you are signed into the system.
- Does the System Verify and hold funds?
  No, it does not.
- Does the system alert me if there is a stop payment on an item or if the check has been reported missing or stolen?
  No, it does not.
- Will I need a separate Internet connection to run the remote deposit capture system scanner?
  No, you won't need one to run the scanner, however you will need a readily reliable available high-speed internet connection to your computer to access Business Online Banking to submit your items to the Bank.

POSITIVE PAY SERVICE

As you issue checks, simply send us a file that contains check information using our Business Online Banking Service. You can also enter this information for single checks directly into our Business Online Banking Service if you have a low volume of checks, want to void a check, or update a manually prepared check – even if it's replacing one already issued.

File import is to occur no later than checks are issued. Best practice for file input is file should be input 24-hours before checks are issued. The system requires CSV format with one line for the header. There should be no special characters, including dollar signs or brackets. Decimals do not count as a special character or have a negative effect. The file should have five fields including check number, date (using slashes, no hyphens), payee, the account number the check is drawn on, and the check amount, in that order.

We compare the check issued data to checks being presented for payment against your account. If there are any exceptions, you are notified by 8:00 AM EST each business day via e-mail, with a reminder email later at 9:30 AM EST. This allows you to go online and view the exception items so you can make a pay or no pay decision. The Positive Pay Exception Review Cut-Off time is noted above. After the cut-off time, any items without a decision (pay or no pay) will automatically be processed as a valid item.

All check issued information provided using Positive Pay is systematically passed on to our teller line, therefore if an altered check is presented at any Solvay Bank teller window then it will not be cashed.

WIRE ORIGINATION SERVICE

Wire transfers are attractive to business customers and consumers because they allow funds to settle same day. It's important to exercise extra caution before completing a wire transfer. The transfer speed, potential size and the inability to recover funds once they are wire transferred to the destination institution all leave the company initiating the wire vulnerable to significant risk. Company will be responsible for self-edification regarding the industry and due diligence of transmitting wire request

Funds Availability

Company agrees transfer requests will not exceed the collected balance in Account nor the granted and agreed-upon limits. A hold will be placed on the Account from which the Wire Transfer is to be made in the amount of the requested Wire Transfer on the date the request is processed by Bank. Bank may not send wires in the case of insufficient funds in the Account or inability to verify the wire with you or Company. If Bank elects, however, to make any transfer that exceeds the collected balance, Company/Individual shall remain liable for any amount transferred in excess of the collected balance in the account.

Transfers Rejected by Bank

Bank reserves the right to reject any Wire Transfer instruction as Bank shall reasonably determine in its sole discretion. In the event Bank rejects any such Wire Transfer instruction, Bank may notify you of any such action by any means reasonable under the circumstance, which need not be in writing. Bank may cancel a Wire Transfer request if it determines that the recipient(s) or any party to the transaction are blocked by OFAC or other restrictions.

Call Backs

Company understands any request to initiate a wire transfer may require a call-back confirmation between Bank and company, in accordance with Bank procedures. Call-back verifications will be made to an authorized individual other than the authorized individual initiating the transfer request.

System Availability

In the event the service is not available, Company may initiate a wire transfer by delivering a Wire Transfer request in person to Bank or via mail, providing the request is complete and has been signed by an authorized representative. Instructions must be complete and include all information required by bank, including, but not limited to, complete name and address of recipient, beneficiary financial institutions, and receiving financial institutions as well as international correspondent banks if applicable.

SECURITY

Security Procedures

Bank recommends Company establish prudent security standards and policies that include proper safeguards to protect the confidentiality of all User IDs and passwords that are assigned to Company for initiating transactions using Business Electronic Services. Any transaction initiated or authorized using a valid combination of User ID and User password will be considered authentic, valid and binding by Company and Solvay Bank. If Company suspects or believes any such information has been compromised, it shall immediately contact Solvay Bank. It is the responsibility of the Company to notify Bank in writing of any changes to those individuals designated as Business Electronic Services Authorized Representative for the Company.

Secure Environment

The Company is solely responsible for providing a secure environment to conduct business with Bank while accessing our Business Electronic Banking Services. Company is required to adopt internal control procedures to protect the integrity and security of Company's access to the system. The Company is also responsible for the accurate creation, modification, and deletion of account information maintained within any of the Business Electronic Banking Services, and on any personal computer(s), mobile device(s) or network(s) used for accessing Business Electronic Banking Services.

The Financial Institution uses industry standard practices to guard the security of Company's transactions and data. However, the Financial Institution does not directly monitor Company's electronic systems and network connections for which Company agrees to accept the entire responsibility. Any electronic transactions submitted through the Bank system using the accepted log on, password, or other security measures are deemed transactions authorized by Company.

It is essential that Business Electronic Banking Service users utilize proper computer security practices. Below are some tips regarding computer security for businesses.

- **Assess Your Risks —** Before you can begin to secure your electronic assets, assess what risks you face based on what data you store and to what degree a system compromise would impact your business. In today's world, a computer system compromise would drastically affect most businesses. Identify the risks and proceed to implement the appropriate controls. Conduct these risk assessments periodically. Business accounts do not receive the same protection as consumer accounts due under Regulation E, which is why it is very important for businesses to protect electronic assets.
- **Implement Dual-Control —** Our business internet banking service offers a dual control feature. Under dual control, all transaction requests must be submitted by one user and approved by another user before processing. This security control can greatly reduce the likelihood of fraud if the transaction is initiated and approved on two different computers. We highly recommend that you consider this feature and please contact us if you think it is right for your business.
- **Stand-Alone Machine or Limited Browsing —** If your employees have access to surf the internet on their work computer, they are exposing your computer system to additional risk. Consider limiting browsing privileges or establishing a machine that will strictly be used for online banking. Ensuring that the computer is only used for online banking will drastically lower the chances of it becoming compromised via an infected e-mail or website.
- **Firewall —** A firewall prevents unauthorized access to your business computer system by restricting allowable communication. Most operating systems have a built-in firewall feature, but you still need to verify that a firewall is indeed present and that it is turned on. Firewall programs are also readily available from security software providers and are often included when a business security suite is purchased.
- **Malware Protection / Anti-Virus Software —** In addition to a Firewall, all computers on your business network should have anti-virus and anti-spyware programs installed. These programs detect and respond to threats that may reach the computer through an e-mail attachment or website. Malicious software, also known as malware, such as computer viruses or spyware, can be used to collect confidential information or even to take control of the entire computer. Consider purchasing a business security suite from a security software developer.
- **Update and Patch All OS, Business, & Security Programs Regularly —** The security software protecting your business will be ineffective if it is not routinely updated. Any program your employees use, especially operating systems and web browsers, need to be updated and patched to protect against new threats.
- **Monitor Account Activity —** If fraud does occur on your business accounts, it is important to catch it as soon as possible. At a minimum, check your accounts daily for unauthorized activity. Contact us immediately if you notice suspicious activity on a business account.
- **Ongoing Employee Education —** Employee education is one of the most effective ways to be protected against cyber fraud. Employees should be trained to be wary of potential phishing scams such as unsolicited phone calls or emails requesting information, pop up messages, and unfamiliar links or attachments. Changes in PC activities and performance such as a differently procedure for log in or a slowed system should be identified by your employees and notification sent to your IT professionals. Use of email encryption by employees also decreases risk.
- **Additional Tips**
  - Enforce a strong workstation password policy
  - Do not send confidential information through unencrypted e-mail
  - Shut down or disconnect computers from the internet when not in use
  - Backup your data