Webster Web-Link®
Browser & Security Information

Contents

Webster Web-Link®
Browser & Operating System Requirements

Webster Bank requires IBM Security Trusteer Rapport be running on all devices used to access Web-Link.
To see a complete list of compatible Operating System (OS) and Browsers*, visit:
Rapport Operating System Requirements Rapport Browser Requirements

Certified Web-Link Resolution Requirements:

- 1024 x 768
- 1680 x 1050

Supported Web-Link Desktop/Laptop Browsers:

- Microsoft Edge – EdgeHTML 12, 13, 14
- Mozilla Firefox 49 – 52 (32bit) (Windows)
- Mozilla Firefox 48 - 50 (Mac)
- Mozilla Firefox ESR 38.7, 38.8 and 45.0
- Google Chrome 49 (Vista Only)
- Google Chrome 54, 55, 56, 61, 62
- Safari 7, 7.1, 8, 9, 9.1, 10
- Windows 7, 8, 10

How To Upgrade Browsers:

- Visit Mozilla.com for Firefox, Google.com for Chrome, or Safari.com for Safari, and follow the prompts to download the latest browser version.

Supported Operating Systems (OS)* for Web-Link:

Windows:

- Required OSs - Windows Vista, Windows 7, Windows 8 and 8.1, Windows 10 & Windows Server 2003/2008/2012 (32 and 64 bit, R1 & R2)
- Required CPU - Intel Pentium 800MHz or better
- Required Memory - Minimum 1024MB RAM

Mac:

- Required OSs - Mac OS X Mountain Lion (10.8), Mac OS X Mavericks (10.9), Mac OS X Snow Leopard (10.6) and X Lion (10.7), Mac OS X Yosemite (10.10), Mac OS X El Capitan (10.11), Mac OS X Sierra (10.12) , Mac OS High Sierra (10.13), Mac OS Mojave (10.14)
- Required CPU - Intel Core or better
- Required Memory - 512MB RAM

Supported OS and Devices for Web-Link Mobile:

iOS:

- Supported Operating Systems - iOS 9.x to 14.x
- Supported Hardware - iPhone 4S to XS Max; all iPads - excluding 1st Gen; iPod Touch 4G and New

Android:

- Supported Operating Systems: Android OS 5.1x to 11.x
- Supported Hardware: Including but not limited to Samsung, Galaxy S6 & Tab 3, Motorola XOOM, Nexus 6P, 7 (2012), & 10

Some browsers may no longer be supported by their manufacture, and Webster recommends that such browsers not be used
*Compatible OS and Browsers are subject to change without prior notice.

Webster Web-Link®
Fraud Protection Tools

1. What security layers are in place when you access Webster Web-Link?

In addition to firewalls and encryption, when you access Web-Link, there are multiple layers of security in place, each designed to guard against different threats:

- **Entry of Company ID, User ID and Password**
- **IBM Security Trusteer Rapport (Rapport)** A security software that Webster requires be running on all desktop devices that access Web-Link. It is not an anti-virus solution. Instead, it targets financial malware and complements anti-virus solutions you should have running on all devices. Rapport does not target other forms of malware, such as ransomware. For a full list of what Trusteer Rapport protects against, visit http://trusteer.force.com/PKB/articles/en_US/FAQ/Which-attacks-rapport-protects?l=en_US
- **Multi-Factor Authentication (MFA).** When you enter your login credentials, MFA authenticates you by using multiple security and validation procedures. For example, when you log in from a new device for the first time, you will be prompted to answer one of your Security Questions that you selected when you first enrolled. This is because MFA recognizes you are on a new device

When you access Web-Link from a mobile device, your banking session includes a dedicated layer of security from IBM.

---

2. What payments fraud PROTECTION tools are available via Web-Link?

- **Out of Band Authentication (OOBA).** A security method in which two separate networks work together to authenticate an online banking user. Referred to as SureKey, it is an optional security layer that organizations can require for all users entitled to originate ACH and Wire payments, or internal transfers from Web-Link.
- **Dual Control for ACH and Wire payments processing.** A combination of dual control and multiple computers (one for entry and one for release, ideally with no email or general internet access) protected by both anti-virus and Rapport are some of the most effective tools to protect against fraud
- **Cash flow security in layers.** We recommend dedicated receivable, operating and disbursement accounts
- **Establish ACH and Wire limits** to meet your business needs
- **ACH Positive Pay alerts** you via Web-Link of potentially fraudulent debits presented against your account. It matches incoming ACH debits against your authorization instructions and allows you to make pay/return decisions online. We strongly recommend you immediately enroll in ACH Authorization Rule Status Alert: Tools. Manage. Alert.Settings.Create Alert. See the Credit Alerts Guide
- **Check Positive Pay.** A highly effective fraud control service that alerts you via Web-Link, of potentially fraudulent checks drawn on your account . See the Check Positive Pay Guide for recommended alerts.
- **Security and Optional alerts.** To help you detect and protect against fraud. These alerts are sent automatically when a particular event occurs in Web-Link . However, there are also important optional alerts. See alert section of the Client Info Center.
- **Recommend daily review and reconciliation of accounts**
- **Guardian Analytics.** We use a behavioral-based fraud detection technology to protect the security of your high-risk transactions. When an ACH or Wire payment is released or received on Web-Link, this Risk Engine monitors, evaluates the characteristics of the transaction for out of the ordinary conditions that could indicate fraud.
- Dual-control for Template creation, or establishing new recipients

Webster Web-Link®
Fraud Protection Tools

3. What else can we do to help you guard against threats?

With the assignment of a Company System Administrator (CSA) by an authorized signer from your organization, the CSA is responsible to establish and maintain user level entitlements, including limits to all the functions granted to your organization during the implementation process. Regular reviews of users' entitlements and limits helps to ensure the right level of permissions are in place.

Beginning on page 5 is a Fraud Awareness & Risk Management Checklist. We recommend you review this regularly. Among other things, it provides tips on how to:

- Protect your identity and the devices used to access Web-Link
- Guard against Business Email Compromise scams
- Conduct risk assessments
- Protect your information security.

Consider attending a Webster hosted or sponsored fraud prevention seminar to stay abreast of changes in the fraud landscape.

4. When and how may Webster contact me?

In addition to calls from your dedicated Client Support Specialist and assigned Webster Banker, we may need to communicate with you about your account(s) via email. Please make sure your current email address registered in Web-Link is current. As needed, other messages will be sent via Web-Link's Banner Messages i.e. holiday closings, service issues, outages, or fraud awareness alerts

Important note: Webster will ***never*** ask for your PIN or account information in any email or expose any sensitive information in any email communications, such as: full account numbers, passwords and social security numbers.

5. What are the resources where more information can be found?

- General Master Service Agreement (MSA)
- Product-related Terms of Service (TOS)
- Fraud Awareness & Risk Management Checklist
- Client Information Center

6. Who should I contact for suspicious account activity?

If you receive a suspicious email, contact your Relationship Manager immediately so we can monitor the account and activity with additional scrutiny. If you did not act on it, forward it to reportfraud@websterbank.com. A report should also be filed with the FBI (New Haven: 203.777.6311) or the FBI website: www.ic3.gov.

If you initiated a fraudulent transaction, immediately contact Webster. We will flag the fraudulent account and attempt to recover funds. A report should be filed with the FBI.

As always however, you can contact your Client Support Specialist with any questions.

Fraud Awareness & Risk Management Checklist

81% of organizations experienced attempted or actual payments fraud.* Your organization can't afford to be disrupted by having funds stolen by criminals or by downloading malicious software. To help make sure you have secure fraud controls in place to protect your organization's data and finances, review this checklist on a regular basis.

Protect Your Credentials

- ❑ Do not share account or log-on credentials
- ❑ Use smart, easy to remember, hard to guess passwords with a mix of upper and lowercase, special characters and numbers i.e. $GoAway2manyHackers! Something that cannot be socially engineered (children birthdates, favorite food)
- ❑ Disable user IDs/passwords during leave/vacation
- ❑ Never use "save ID/password" on websites where sensitive and/or financial data is accessed/stored
- ❑ Consider privacy overlays on computer screens, especially log-on credentials
- ❑ Store passwords securely (not in drawer or under keyboard)

Protect Your Computer and Mobile Devices

- ❑ Do not download or open attachments from unfamiliar file sharing sites or click on links in an email unless you're expecting them or recognize the sender
- ❑ Review internet security regularly; validate best practices
- ❑ Back-up files regularly to off-site, non-networked storage

Protect Your Staff and Organization

- ❑ Secure your workplace and access to paper files by non-employees (i.e. trash)
- ❑ Limit authorization to employees who need it
- ❑ Segregate duties within accounting department
- ❑ Conduct surprise audits
- ❑ Conduct periodic risk assessments and controls evaluation
- ❑ Rotate banking duties among staff to prevent collusion
- ❑ Review system access privileges regularly
- ❑ Educate employees, vendors, temps, and customers on cyber security issues, external dangers, internal controls, protection of information and systems. Ensure understanding and compliance
- ❑ Keep your senior management aware of cyber security activities and management
- ❑ Do not embed signatures in emails or put executive email addresses on your website

Protect and Control Financial Transactions

- ❑ Use dedicated and protected computers. One per user, follow Dual Control procedures, including online ACH originations/file transmissions, Fed wires, check processing and Remote Deposit**
- ❑ Reconcile daily/monthly (separate duties - staff that issue payments vs. those that reconcile)
- ❑ Validate email instructions to place a wire or to change any recipient, address or account information with a call to a known phone number on file or in person, before processing
- ❑ Scan email addresses for correctness (2 n's form m)
- ❑ Void/secure checks remotely deposited
- ❑ Shred deposited items after predetermined timeframe
- ❑ Convert paper-based payments to electronic payments
- ❑ Review and update signature cards annually
- ❑ Physically turn off your computer (not automated timeout)
- ❑ Do not share, publish or provide your Employer or Employee ID numbers unless absolutely required and validated
- ❑ Do not include sensitive information such as SSNs in payroll file transmissions
- ❑ Ensure negotiable documents have a control # managed under Dual Control

Note: There is a difference between when checks are deposited drawn on other banks, when funds are made available (per regulations) and when funds are "good" funds, and therefore collected.

Protect Your Check Supply

- ❑ Use an established vendor. Use a unique check style per account for easy differentiation
- ❑ Use stock with pre-printed numbers to identify missing checks
- ❑ Incorporate security features into your check design
- ❑ Monitor orders and inform supplier if not delivered in a reasonable time
- ❑ Use secure storage with controlled access for printing and Remote Deposited checks, endorsement stamp and cancelled checks
- ❑ Never sign checks in advance

*2020 Annual Payment Fraud and Control Survey, Association for Financial Professionals. **Restrict access to these computers and specific access sites. Ideally with no email or general internet access.

Fraud Awareness & Risk Management Checklist

Have a Comprehensive Information Security Policy

Your IT experts can upgrade an existing policy or create one:

- Clear security objectives to preserve confidentiality, integrity and availability of information
- Detail network access for employees/contractors
- Formal agreement from all applicable parties
- Logical and physical access controls
- Deploy operating system network software, anti-virus and security certification verifications and patches regularly
- Implement a comprehensive Unified Threat Management System (UTM), inclusive of Intrusion Protective Software (IPS)
- Ensure network routers are protected

Conduct Periodic Risk Assessments

Discover, correct and prevent security problems. Involve representatives from all applicable parties. Include:

- System inventory, list all components, policies/procedures, and details of its operation
- Risks (i.e. reputation, operational or technology), severity of impact and likelihood of occurrence
- Safeguards for controlling threats/vulnerabilities, recommended actions, approximate effort/timeframe and level of residual risk remaining
- Proactive vulnerability testing
- Resources for incident response, separate from those in vulnerability analysis and security controls. Ensure emergency response teams have a contact list, including back-ups and day/evening info
- Evaluation and adoption of cyber liability, privacy liability and/or network security to mitigate IT fraud-related expenses
- Disaster recovery (testing) plans: What if the internet was down, if applications, files and other web-based programs were impacted, destroyed or not available? Be aware of services to your organization that are web-enabled

Webster Treasury & Payment Solutions provides cash management services that can help you reduce risk:

Online and Mobile Banking

- ❑ 3-point security authentication at log-in
- ❑ Review account(s) daily
- ❑ Set alerts to be notified of any changes:
  - ❑ Check Positive Pay Exception Item
  - ❑ ACH Positive Pay Exception and Batch Release
  - ❑ Wire Release
  - ❑ Password Change or Reset
  - ❑ Update Security Challenge Questions
  - ❑ Out of Band Authentication

Paper Transactions

- ❑ Use Check Positive Pay, with default of return
- ❑ Use Check safekeeping policies – truncate or shred/destroy cancelled checks
- ❑ Request images of paid/deposited checks
- ❑ Set-up Check Block to stop all checks from debiting
- ❑ Lockbox Services – segregation of duties

Ach and Wire Transactions

- ❑ Adopt a Dual Control environment
- ❑ Ensure entitlements and transaction limits correspond to business need
- ❑ Use ACH Positive Pay - ensure only authorized originators debit your account up to a predetermined amount; or block all debits to your account

Account Opening and Maintenance

- ❑ Minimize number of accounts to reduce fraud risk
- ❑ Use unique serial number ranges for specific purposes within one account instead of additional accounts
- ❑ Segregate access to accounts that are at greater risk

If you do experience a malware attack, do not turn off your device. Disconnect from network.

If you feel that you have received a fraudulent or suspicious email from Webster Bank:

- Forward the email to reportfraud@websterbank.com
- Or, call Webster Bank's Security Hotline at 1.800.966.0256, 7:00 am to 10:00 pm, 7 days a week