Consumer Online and Mobile Banking Agreement

Effective December 15, 2026

1. About This Agreement

This Consumer Online and Mobile Banking Agreement ("Agreement") governs your use of Achieva Credit Union's consumer Online Banking and Mobile Banking services (together, the "Service"). In this Agreement, "you" means each consumer member who enrolls in or uses the Service, and "we," "us," and "our" mean Achieva Credit Union.

The Service is for personal, family, or household use. It does not cover commercial online banking, treasury management, or other business services. Some features are available only through Online Banking or only through Mobile Banking.

This Agreement supplements the agreements and disclosures that govern your accounts, including the Universal Account Agreement and applicable deposit, loan, credit card, rate, and fee disclosures ("Account Agreements"). If this Agreement conflicts with an Account Agreement about the Service, this Agreement controls to the extent of the conflict.

Accepting This Agreement

Before using the Service, you must consent to electronic records and disclosures and accept this Agreement. Your electronic acceptance or use of the Service has the same effect as your handwritten signature. Each time you log in or use the Service, you confirm your continuing acceptance of this Agreement.

2. Electronic Records and Disclosures

By accepting this Agreement, you consent to receive disclosures, notices, agreements, and other information about the Service electronically and to use electronic records and communications. This consent is required to use the Service and applies to every account you enroll now or later.

We may deliver information by email, text message, a message within the Service, our website, the Mobile Banking app, an electronic account statement, or another electronic method you authorize. Electronic notices may include notices about payments, transfers, account activity, Service changes, and amendments to this Agreement.

Technology You Need

You must have internet or mobile-data access, a valid and current email address, and current software that can open and save PDF and HTML documents and supports Transport Layer Security

encryption. Mobile Banking requires a compatible mobile device and the current version of our Mobile Banking app. Keep your operating system, browser, PDF reader, and app updated.

By enrolling, you confirm that you can access, view, print, or electronically save the records we provide. If you cannot do so, do not enroll in or use the Service.

Keeping Your Contact Information Current

You are responsible for keeping your email address, mobile number, mailing address, and other contact information current. Call us at (727) 431-7680 or write to Achieva Credit Union, P.O. Box 1500, Dunedin, FL 34697 to report a change. To help avoid delayed statements, provide an email-address change at least three Business Days before the last Business Day of the month.

If an email is returned as undeliverable, we may change your statement delivery to paper and charge the paper-statement fee shown in the Consumer Schedule of Fees. You will need to provide a correct email address and re-enroll in electronic delivery, if available.

Paper Copies and Withdrawing Consent

We do not charge for electronic delivery. You may request a paper copy of a previously delivered electronic record by calling or writing us; applicable copy fees may apply. You may withdraw your consent to electronic delivery at any time by calling or writing us. If you withdraw consent, we may end your use of the Service and may not process future-dated payments that have not yet been processed.

3. What You Can Do

You may enroll eligible personal deposit, loan, and credit card accounts (“Eligible Accounts”). Available features may include viewing balances and transaction history, locating branches, transferring funds, making loan or credit card payments, placing eligible stop-payment orders, using supported financial software, and depositing checks through Mobile Banking.

Bill Pay, external account transfers, person-to-person payments, and certain other services may require separate terms. We may add, change, limit, or remove features or access methods at any time. Features may differ between Online Banking and Mobile Banking, and we may refuse a transaction requested through the Service.

Service Availability

We will use reasonable efforts to make the Service available with minimal interruption, but we do not promise uninterrupted access. Maintenance, internet or telecommunications outages, emergencies, device limitations, network conditions, geographic restrictions, or events beyond our control may make the Service unavailable.

Messages and Email

You may use email for general questions or feedback, but you may not use ordinary email to initiate account transactions. Do not include account numbers or other sensitive information in ordinary email. Use the secure messaging feature within Online Banking when available.

Alerts

We may offer optional account alerts by email, text message, or push notification, and we may send certain security or account alerts that you cannot turn off. By enrolling in alerts or giving us a mobile number, you agree to receive alerts at the contact points you provide, including automated text messages. You are responsible for keeping those contact points current and secure.

Alerts are a convenience and do not replace reviewing your account activity and statements. Alerts may be delayed, not delivered, or inaccurate because of technical problems, carrier issues, or events beyond our control. Alerts are not encrypted and may include limited account information that anyone with access to your device or email may see. We do not charge for alerts, but your mobile carrier's message and data rates may apply. To stop text alerts, manage your alert preferences within the Service or call (727) 431-7680.

Fees

We currently do not charge a fee merely to access Eligible Accounts through the Service. Transaction fees may apply as disclosed in your Account Agreements, the Consumer Schedule of Fees, or within the Service before you complete a transaction. We may add or change Service fees after providing any notice required by law. Your internet, mobile, or other third-party provider may charge you separately.

4. Protecting Your Accounts

Your login ID, password, passcode, security token, biometric sign-in, and other authentication methods are your "Access Credentials." Keep them, your account numbers, and your account information confidential. Use strong credentials, change them when appropriate, and do not write them where others can find them. You should not share your Access Credentials with anyone. If you give your Access Credentials to another person, app, service, or AI Agent, or let them use a device on which you are signed in, you authorize them to access your Eligible Accounts. To the extent permitted by applicable law, you are responsible for transactions they make, even if they go beyond what you intended, until you tell us they are no longer authorized and we have had a reasonable opportunity to act. We will never contact you to ask for your password or a one-time passcode.

We may use challenge questions, one-time codes, device information, or other methods to verify your identity. We may deny access if we cannot verify you.

Trusted Devices and Additional Verification

We may require you to use our Mobile Banking app, to register a device as a trusted device, or to complete additional identity verification before you can sign in, add a new device, change security settings, or complete certain transactions, including transactions requested through an AI Agent or other third-party service. We may limit, delay, or deny access or a transaction until verification is complete, and we may remove trusted-device status from any device. You are responsible for the security of each device you register. Remove a device from your profile before you sell, give away, or stop using it.

Password Managers and Other Credential Tools

You may use a reputable password manager or other credential storage tool, including one built into your device or browser, to store and enter your Access Credentials for your own use. Protect that tool with a strong master password and multifactor authentication where available, and keep it updated. If the tool lets another person, device, app, or AI Agent retrieve or use your Access Credentials, you are treated as having shared your Access Credentials with them. We do not provide or control third-party credential tools and, except as required by applicable law, are not responsible for their security, availability, or performance.

Mobile Devices and Biometrics

Your primary Access Credentials may be used for both Online Banking and Mobile Banking. We may also allow a passcode or biometric sign-in. If another person's biometric information is stored on a device you use for Mobile Banking, that person may be able to access and transact through your Service. Do not enable biometric sign-in on a shared device unless you accept that risk.

Remove any device that you no longer want connected to Mobile Banking and delete the app when appropriate. Subject to applicable law, instructions authenticated with your Access Credentials may be treated as your authorized instructions.

Lost Credentials, Devices, or Unauthorized Activity

If you believe an Access Credential or device is lost, stolen, or compromised, or that an unauthorized transfer has occurred or may occur, call (727) 431-7680 immediately. Your Account Agreements explain your rights and responsibilities for unauthorized electronic fund transfers. Call us also if you believe an AI Agent or other service you authorized has been compromised, is acting outside your instructions, or should no longer have access.

Errors or Questions

Call the Member Service Center at (727) 431-7680 if you have an error or question about a transfer or Eligible Account. Your Account Agreements explain the procedures and time limits that apply. Nothing in this Agreement limits any rights you have under the Electronic Fund Transfer Act, Regulation E, or other applicable law that cannot be changed by agreement.

5. Transfers and Payments

Available transfer options may include transfers between your Eligible Accounts, transfers to another person's account with us, payments to your loans or credit cards, and advances from an eligible loan or credit card to a deposit account.

Transfers to Another Member

You must provide the correct destination account information. We may set or change limits on the number or amount of transfers. Transfers to another member cannot be canceled after submission. A transfer sent to incorrect account information may not be recoverable.

Loan and Credit Card Payments

Regular payments are applied under the applicable loan or credit card agreement. If a principal-only option is available, it does not satisfy a scheduled payment requirement.

Canceling Scheduled Transactions

You may schedule one-time or recurring transfers, payments, or advances when the feature is available. To cancel, submit the cancellation at least one day before the scheduled processing date. A transfer to another member cannot be canceled after it is submitted.

Insufficient Funds

If an account lacks enough available funds, we may reject the transaction or, in our discretion, complete it and overdraw the account. Applicable overdraft or insufficient-funds fees may apply. Other electronic transactions may receive priority under our processing rules and your Account Agreements.

6. Stop Payments, Records, and Financial Software

Stop Payments

You may place a stop payment on a single check or a range of checks through Online Banking when the feature is available. For a series of checks, call (727) 431-7680. We must receive the order in time to have a reasonable opportunity to act. You must accurately provide the check number, date, amount, and payee. Legal limitations and the stop-payment fee for your account apply.

Transaction Records

Details of transfers and other transactions will be available through the Service and will appear on your regular account statements.

Supported Financial Software

We may allow you to download or access Eligible Account information through supported personal financial software. Availability and functionality may change. Your use of third-party software is also subject to the provider's terms.

7. Mobile Check Deposit

Mobile Check Deposit lets you use a compatible, camera-enabled device to send images of eligible checks to an eligible personal checking, savings, or money market account. You must capture clear images of the front and back, including the magnetic-ink character-recognition line, and provide any information the app requests. Technical information may include your IP address, device identifier, and device location when enabled.

Eligible Checks

Deposit only checks payable to an owner of the receiving account and acceptable under our procedures. Do not deposit:

- Checks payable to someone who is not an owner of the receiving account.
- Checks you issued, or checks drawn on an account on which you are a joint owner or authorized signer.
- Altered checks or jointly payable checks unless all payees are owners of the receiving account.
- Substitute checks, remotely created checks, drafts payable on sight or through another institution, or checks drawn on a foreign bank or payable in foreign currency.
- Undated or postdated checks, or checks dated more than six months earlier.
- Checks with an endorsement that does not follow our instructions.
- Checks previously deposited, previously returned unpaid, or otherwise presented for payment.
- U.S. Treasury checks, state or federal government checks, registered government warrants, traveler's checks, money orders, or checks payable to "Cash."
- Checks transmitted from outside the United States or any item prohibited by our current procedures or your Account Agreement.

We may reject any item or accept it only for collection. We may charge back an item later determined to be ineligible.

Endorsement and Image Quality

Sign the back of the check and add "FOR MOBILE DEPOSIT ONLY AT ACHIEVA CREDIT UNION," or use another restrictive endorsement we instruct you to use. Images must be accurate, complete, and legible. We may reject a deposit if image quality is insufficient.

Receipt and Check Storage

A deposit image is received when we send confirmation, but confirmation does not mean the transmission was error-free, complete, accepted, or credited. Keep the original check for at least 60 calendar days after transmission. After 60 days, destroy it, mark it "VOID," or otherwise prevent reuse. Provide the original promptly if we request it.

Availability, Limits, and Fees

Mobile deposits are not subject to the funds-availability requirements of Regulation CC. Funds generally become available after we receive payment, although we may make them available sooner. We may set deposit amount and item limits and may reject a deposit that exceeds them. Applicable limits and any fee will be shown before submission.

Your Promises

You promise that each item is eligible, each image meets our standards, all information is accurate, you will not submit duplicates or redeposit an original, and you will follow this Agreement and applicable law. You make the same warranties that would apply to a paper-check deposit and agree to reimburse us for losses caused by your breach of these promises.

8. Devices, Software, and Third Parties

You are responsible for your devices, software, internet access, mobile service, and related costs. We are not a party to your agreements with device manufacturers, app stores, internet providers, mobile carriers, AI Agent providers, or other third parties. Resolve problems with their products or services directly with them.

Your devices and communications may be exposed to viruses, malware, spyware, unauthorized tracking, or other attacks. Use current security tools and reasonable safeguards. We are not responsible for advising you about every threat.

Mobile App License

Our licensors and service providers retain all rights not granted to you. Downloading or using the Mobile Banking app means you accept applicable end-user license terms. If you change devices, you may need to reinstall the app. Delete the app if your right to use it or this Agreement ends. We may change app providers or app functionality.

Export Controls

Software and technical data may be subject to U.S. export controls and other trade laws. You agree to comply with applicable restrictions and not export or re-export the software to prohibited persons, entities, or countries.

9. Artificial Intelligence, AI Agents, and Automated Access

This section explains how artificial intelligence and other automated tools may be used with the Service, including AI-powered features we may offer and AI Agents or other tools you choose to use. An "AI Agent" is any software, application, assistant, browser extension, bot, script, or other automated tool, whether or not it uses artificial intelligence, that accesses, reads, or monitors the Service or takes or attempts to take any action in the Service on your behalf, with or without your real-time involvement. Nothing in this section limits any rights you have under the Electronic Fund Transfer Act, Regulation E, or other applicable law that cannot be changed by agreement.

AI-Powered Features We Offer

We may offer features within the Service, on our Website, or through our member support channels that use artificial intelligence, such as a virtual assistant, a chat feature, or a tool that summarizes account activity or answers questions ("AI Features"). When you use an AI Feature:

- **Responses may be inaccurate or incomplete.** AI Features can make mistakes, misunderstand your request, or give information that is incomplete or out of date. Confirm balances, transactions, payment dates, and other important information in the Service or your statements before relying on it.
- **Responses are not advice and do not change your terms.** AI Features do not provide financial, investment, tax, or legal advice. Their responses do not change this Agreement, your Account Agreements, or any rate, fee, or disclosure we provide.
- **You remain in control of transactions.** If an AI Feature helps you prepare a transfer, payment, or other request, review the details carefully before you confirm it. We will process the request as you confirm it.
- **You can reach a person.** You may ask to speak with a member of our staff at any time by calling (727) 431-7680.
- **Your interactions may be recorded.** We and our service providers may record, retain, and review your interactions with AI Features to provide, secure, and improve the Service, to prevent fraud, and to comply with law, as described in our Privacy Notice.

Reporting problems. If you believe an AI Feature gave you inaccurate information, tell us through the Service or by calling (727) 431-7680. If you tell an AI Feature about a suspected error, an unauthorized transaction, or lost or stolen Access Credentials, we will treat that communication as required by applicable law, but please also call us right away so we can act as quickly as possible.

Using Your Own AI Agent

You may choose to use an AI Agent to view account information or to request transfers, payments, or other actions through the Service. Unless we tell you otherwise in writing, AI Agents are not provided, endorsed, or controlled by us, and a third-party AI Agent is not our agent or service provider. We are not required to support any particular AI Agent, and some features of the Service may not work with AI Agents.

When we make available a secure method for third-party access that does not require you to share your Access Credentials (an "Authorized Connection"), you should use it, and we may require AI Agents and other third-party services to use it. Giving an AI Agent your Access Credentials, or letting it operate a device or browser session in which you are signed in, creates additional risk for you, including the risk that the AI Agent or its provider is compromised.

If you choose to use an AI Agent by any method, you agree that:

- **You authorize it.** The AI Agent acts on your behalf. To the extent permitted by applicable law, including Regulation E, any instruction, transaction, or other action taken through the Service by an AI Agent you enabled, whether using your Access Credentials, your signed-in session, or an Authorized Connection you set up, is authorized by you. This applies even if the AI Agent misunderstands your instructions, makes a mistake, malfunctions, or does more than you intended, until you notify us as described below and we have had a reasonable opportunity to act.
- **You are responsible for supervising it.** You are responsible for choosing the AI Agent, deciding what it may do, setting any limits it offers, monitoring its activity, and promptly reviewing your account activity, alerts, and statements. We are not required to determine whether an instruction from an AI Agent matches what you intended.
- **Your information leaves our systems.** Information you or the AI Agent obtain from the Service may be stored, used, or shared by the AI Agent's provider under its own terms and privacy practices, which we do not control. Review those terms before you use an AI Agent. Except as required by applicable law, we are not responsible for how information is used after it leaves the Service.
- **Security steps stay with you.** Do not allow an AI Agent to receive, read, or respond to one-time passcodes, security prompts, or fraud alerts we send you, or to approve sign-ins or transactions for you, unless we have expressly enabled that capability.
- **It must follow this Agreement.** Actions taken by your AI Agent are subject to this Agreement and your Account Agreements, and you are responsible if your AI Agent violates them.

Ending an AI Agent's Access

To stop an AI Agent from accessing the Service, disconnect it through the Service or the Authorized Connection if one was used, change any Access Credentials you shared with it, sign out of any session it can use, and call us at (727) 431-7680. If you believe an AI Agent has been compromised, has acted without your authorization, or has made an unauthorized transfer, call us immediately. Your rights regarding unauthorized electronic fund transfers are described in your Account Agreements.

Our Right to Monitor, Limit, or Block Automated Access

To protect you, us, and other members, we may, subject to applicable law: identify and monitor automated access to the Service; require an AI Agent to identify itself or to use an Authorized Connection; limit how often or how quickly an AI Agent may access the Service; require you to confirm a transaction or complete additional verification yourself; decline or delay a transaction

requested by an AI Agent; and block, suspend, or disconnect any AI Agent, or any type of AI Agent, from the Service. We may take these actions without advance notice when we believe they are reasonably necessary for security, fraud prevention, system integrity, or legal compliance.

Prohibited Automated Activities

Whether or not you use an AI Agent, you may not use, or allow anyone else to use, any automated tool, including an AI Agent, to:

- access or attempt to access any account or information that does not belong to you or that you are not authorized to access;
- bypass, disable, defeat, or interfere with any authentication, multifactor authentication, device-registration, human-verification, rate-limiting, or fraud-prevention control;
- probe, scan, test, reverse engineer, or analyze the security, source code, fraud-detection systems, or infrastructure of the Service;
- copy, scrape, or extract the Service's software, design, interface elements, or other proprietary content (other than your own account information), or use that content to train or improve an artificial intelligence or machine-learning model;
- place an unreasonable load on the Service or interfere with its operation or with other members' use of it; or
- engage in fraudulent, unlawful, or deceptive activity, or impersonate any person.

Right to Suspend or Terminate

If we detect or reasonably suspect activity that violates this section, or that an AI Agent poses a risk to your accounts, to us, or to other members, we may immediately block, suspend, or terminate your access, or the AI Agent's access, to all or part of the Service without prior notice, subject to applicable law. To the extent permitted by applicable law, we are not liable for failed or delayed transactions, fees, or losses resulting from that action.

10. Liability, Warranties, and Disputes

Except where this Agreement or applicable law provides otherwise, the Service, AI Features, and related software are provided "as is" and without warranties of merchantability, fitness for a particular purpose, noninfringement, accuracy, completeness, uninterrupted operation, security, or error-free performance.

To the extent permitted by law, we are not responsible for losses caused by your equipment or software, internet or mobile providers, third-party services (including AI Agents you choose to use), malware, communication failures, or circumstances beyond our control. We are not liable for indirect, special, incidental, consequential, or lost-profit damages arising from the Service.

Except to the extent we are liable under this Agreement, an Account Agreement, or applicable law, you agree to protect and reimburse us and our directors, officers, employees, affiliates, agents, and service providers for claims, losses, liabilities, and reasonable costs resulting from your instructions, your or your agent's acts or omissions (including those of any AI Agent you use), your

disclosure of your Access Credentials to any person or AI Agent, your breach of this Agreement, your misuse of equipment or software, or warranties we must make to third parties because of your transactions.

We may change the Service, fees, or this Agreement. We will provide notice when required by law. Notice of a new or increased fee, and other advance notice when required, generally will be provided at least 21 days before the effective date. A security-related change may take effect immediately, with notice afterward when required. Continued use after the effective date means you accept the change.

We may send notices electronically as described in this Agreement or by mail or another legally permitted method. A notice posted within the Service is considered given when posted; a notice sent to your email address or device is considered given when sent.

We may suspend or terminate all or part of the Service at any time, subject to applicable law. If you do not access an Eligible Account through the Service for 90 consecutive days, we may suspend or disconnect access and related alerts. We may also terminate Mobile Check Deposit if you violate this Agreement, use it unlawfully, or use it inconsistently with another agreement with us.

You may end Online Banking or Mobile Banking by calling or writing to the Member Service Center. For Mobile Banking, also unregister your device and remove the app. Terms that by their nature should continue after termination will remain in effect.

This Agreement is governed by federal law and regulations and, where applicable, Florida law. Disputes about the Service will be resolved under the dispute-resolution provisions in your Account Agreements.

11. Definitions

Access Credentials: Any login ID, password, passcode, token, biometric identifier, or other method used to identify you or access the Service.

Account Agreement: Any agreement or disclosure governing an Eligible Account, including applications, rate and fee schedules, deposit agreements, credit card agreements, promissory notes, and loan agreements.

AI Agent: Any software, application, assistant, browser extension, bot, script, or other automated tool, whether or not it uses artificial intelligence, that accesses, reads, or monitors the Service or takes or attempts to take any action in the Service on your behalf.

AI Features: Features of the Service, our Website, or our member support channels that use artificial intelligence, as described in Section 9.

Authorized Connection: A secure method we make available for third-party access to the Service that does not require you to share your Access Credentials, as described in Section 9.

Business Day: Monday through Friday, excluding Federal Reserve holidays and other days financial institutions are legally closed.

Deposit Account: A personal checking, savings, money market, or other deposit account enrolled in the Service.

Eligible Account: A personal Deposit Account, loan, or credit card account that we permit you to enroll in the Service.

Mobile Banking: The consumer banking services available through a permitted mobile device and our Mobile Banking app.

Mobile Device: A compatible phone, tablet, or similar wireless device used to access Mobile Banking.

Online Banking: The consumer electronic banking services available through our website, including supported features governed by this Agreement or separate terms.

Service: Online Banking and Mobile Banking together, including consumer features we make available under this Agreement.

Website: Achieva Credit Union's website and related pages used to access Online Banking.

12. Contact Us

Member Service Center
Phone: (727) 431-7680
Achieva Credit Union
P.O. Box 1500
Dunedin, FL 34697

Save or print a copy of this Agreement for your records.