Technology and Information Protection (T.I.P.)

Farm Credit Illinois is committed to protecting your financial information both online and off. The following procedures are in place to keep your funds and information secure.

Online Banking

- Transferring of Funds Externally
  - In order to transfer money to third parties, contact your local branch office to request an Opt-In Agreement Form. Once completed, this form authorizes FCI to disburse funds to the external parties identified.
- Transaction Activity
  - All transactions on your loan(s) can be viewed anytime through Online Banking.
- Positive Pay Protection for Sight Drafts
  - Positive Pay protection is available through Online Banking. To enable this feature, you must import all sight drafts into Online Banking. If a sight draft is presented to FCI for payment that is not imported into the system, you will be notified. The sight draft will not be paid unless you affirmatively instruct FCI to pay the draft.

Electronic Disbursement Block

- Before processing any third party electronic payment (input suppliers, insurance companies, tax payments), FCI will notify you to determine if the disbursement is authorized. If you know of certain third party vendors that will continually debit your account, you may request FCI allows those disbursements without further authorization.

Member Identification Verification

- When requesting a disbursement of funds or sensitive information via phone, email, or fax, FCI will take appropriate measures to verify the request is from you, the account holder or other authorized party.

Keep Yourself Protected

- Under the terms of FCI's loan documents, you have various responsibilities to ensure loan funds are not misappropriated, misdirected, or otherwise misused. Please carefully review loan documents and other agreements to understand your obligations and liabilities.
- To protect your funds and information, FCI recommends each member:
  - Keep sight drafts in a secure place to avoid any forgeries or lost or stolen information.
  - Create and keep a strong, secure password; do not use names or dates.
  - Keep anti-virus software current on all computers.
  - Avoid clicking on any suspicious links in emails or while surfing the Web.
  - Routinely review account activity – this can be done daily via Online Banking, or monthly via Monthly Member Statements.
- Notify FCI immediately if you become aware of any information or irregularity that may indicate your information or account security has been, or may be compromised.
- Emails sent online can be stolen by others; think twice before sending confidential information.