The Fund® DON'T BE A FRAUD MAGNET!

Minimum Standards - S.E.C.U.R.I.T.Y.

Seller & Borrower Verification

ID: Obtain a valid government-issued color ID and closely scrutinize for authenticity.

Independently Verify Transaction with Property Owner: Confirm independently with the property owner in vacant land or absentee owner situations that the upcoming transaction is legitimate.

Escrow Protector

Independently Verify Payoff & Wire Transfer Instructions (WTI) with a Trusted Source: Beware of unsolicited payoff/WTI and compare for consistency. Beware of changes to routing & account numbers.

Encrypt Wire Communication: Encrypt emails containing WTI or Personal Information (PI).

Avoid Sensitive Terms in Email Subject Lines: (For example, a subject line using "Wire Instructions" is highly susceptible to spoofing and phishing attacks).

Track the Transaction: Keep track of transfers and monitor for any last-minute changes. Track receipt of disbursements (payoffs, insurance, seller proceeds).

Common Sense

Trust Your Instinct: Pause proceedings if there is a rejected wire, substituted unknown notary, or other irregularities. Be cautious of any last-minute changes, especially with vacant land, absentee owners, and foreign sellers.

Documents: Compare signor(s) locations on executed documents (deed/mortgage) with their ID document(s), and compare handwriting & signatures for similarities (witnesses, notary, grantor).

Utilize Secure Protocols

RON Service Providers: Use industry trusted and known RON platforms which incorporate KBA and other ID verifications.

Email Services Providers: Use secure email providers, avoiding public platform providers like Gmail, Yahoo, AOL, etc.

Cybersecurity Measures: Implement strict access controls.

Routine Training

Train Staff: Regularly update staff on fraud and anti-fraud techniques and encourage review of Fund education materials.

Practice Drills: Run drills and action plan rehearsals, including simulated test phishing emails to keep staff alert.

Incident Response Plan (IRP)

Incident Response Plan: Develop and maintain a strong plan with instructions, critical contacts including your bank's security officer, action items, and E&O carrier info.

Immediate Fraud Response: Inform outgoing and receiving banks immediately upon detecting fraud. Diligently work to recall wires.

Take Charge of the Closing

Trusted Sources: Control the closing process. Rely on trusted sources and known notaries.

RON: Use RON notary or require execution of documents with a known attorney or notary for signors who are not present and are unknown.

You

Stay updated on fraud trends and anti-fraud techniques.

Detect and Prevent Fraud: The responsibility ultimately lies with you. Everyone is counting on you to prevent fraud. You are in the best position to detect and thwart fraud.

Protect Yourself: These policies are essential to protect your business and livelihood.

The Fund® DON'T BE A FRAUD MAGNET!

Strongly Recommended - P.R.O.T.E.C.T.

Passwords
- Use strong passwords and change them frequently.
- Adopt ALTA's best practices where appropriate.

Records
- Secure records and purge Personal Information (PI).
- Transfer closed files with PI from internet-exposed servers to an external hard drive or other secured storage.

Operations
- Avoid personal email for work communications.
- Refrain from using open networks.
- Follow secure protocols to protect PI and other sensitive information.
- Regularly update your system to include all security patches by enabling automatic updates, using reliable antivirus software, keeping all software up-to-date, and backing up data to encrypted servers.
- Obtain and scrutinize a second valid government-issued ID.
- Consider sending a check instead of a wire but be aware of check washing risks.

Tools
- Use third-party vendors for wire transfer security, identity, and seller/borrower verification (e.g., CertifID, TLO Skip Tracing, Persona, Verisoul).
- Consider services that confirm bank account ownership.

Errors & Omissions Insurance
- Review and understand coverages and limitations of your E&O policy. Analyze to maximize protection for potential loss and actions taken as a closing agent.
- Ensure your office adheres to policy prerequisites and conditions for claims.
- Promptly review and comply with your E&O policy concerning notice obligations.

Cybersecurity Insurance
- Acquire cybersecurity insurance to cover matters excluded by E&O insurance.

Technology
- Implement Multifactor Authentication (MFA) across all accounts and devices.
- Utilize Positive Pay for escrow accounts.
- Use FaceTime or similar applications to secondarily verify ID photos with unknown seller/borrower on camera.