

Closing Day Wire Fraud Defense Checklist

Large sums and tight deadlines make real estate closings a top target for wire fraud. Use this checklist to protect your clients' funds before, during and after every wire.

THE GOLDEN RULE



Wiring instructions never change by email. Verify every change by phone, using a number you already have on file.

1 Before closing

- ☐ **Set expectations in writing.** Say in your engagement letter and first email that wiring instructions will never change by email.
- ☐ **Turn on multi-factor sign-in** for every firm email account, including paralegals and assistants.
- ☐ **Send instructions securely** through a client portal or encrypted email, never a plain email reply.
- ☐ **Verify payoff letters** by calling the lender at a number from its official website, not the letter.
- ☐ **Collect phone numbers early** for buyer, seller, lender and broker, confirmed in person or at intake.

2 On closing day

- ☐ **Call back on every wire.** Confirm account and routing numbers by phone before any funds go out.
- ☐ **Treat any change as a red flag.** A new bank, new account or "updated" instructions means stop and verify.
- ☐ **Check the address, not the name.** Look for look-alike domains and a different reply-to address.
- ☐ **Require two people** to review and approve every outgoing wire.
- ☐ **Confirm receipt the same day** by calling the recipient at a number you already trust.

3 After the wire

- ☐ **Confirm funds arrived** by phone within hours, not days.
- ☐ **Check email for hidden rules.** Unknown forwarding rules are a sign of a hacked account.
- ☐ **Store files securely.** Encrypt closing files and shred paper you no longer need.

⚠ Stop and call if you see...

- Last-minute wiring changes
- Pressure to rush or keep it quiet
- An account name that doesn't match
- A bank in an unexpected place
- An email that's one letter off
- A sender who won't take a call

If a wire goes wrong: your first hour

Speed matters. The sooner the bank and the FBI know, the better the chance of getting funds back.

1 Call your bank's fraud line. Ask them to recall the wire and contact the receiving bank now.

2 Report it to the FBI at ic3.gov, and call your local FBI field office.

3 Save the evidence. Don't delete anything. Keep emails, headers and wire records.

4 Lock down email. Reset passwords, remove unknown rules and call your IT provider.

5 Call your insurers: cyber, malpractice and your title underwriter.

6 Notify the right people, including clients. Review your notice duties under M.G.L. c. 93H.

KEEP THESE NUMBERS AT YOUR DESK

Bank Fraud Line _____

IT Provider _____

Cyber Insurance Carrier _____

Title Underwriter _____

Quick check: is your firm ready?

Massachusetts requires firms that hold residents' personal information to keep a written security program (201 CMR 17.00). Check Yes or No for each.

OUR FIRM...	YES	NO
Has a written security program (WISP), reviewed every year	☐	☐
Uses multi-factor sign-in on every email account	☐	☐
Trains all staff on phishing and wire fraud every year	☐	☐
Has a written call-back policy for any wiring change	☐	☐
Encrypts client data in email and on laptops	☐	☐
Cuts off email access on an employee's last day	☐	☐
Has cyber insurance that covers wire fraud	☐	☐
Knows who to call if a wire goes wrong	☐	☐

8 Yes

Strong foundation. Keep it up.

6-7 Yes

A few gaps worth closing soon.

5 or fewer

Your firm may be an easy target.

HAVE A GAP? LET'S CLOSE IT.

Talk with Secure Future Tech Solutions

We help firms across Rhode Island and Massachusetts stop wire fraud before it starts.

401-537-1170 www.securefuturetech.com

SCAN HERE



This checklist is general information for educational purposes and is not legal advice. Review your firm's obligations under 201 CMR 17.00, M.G.L. c. 93H and your professional rules.