SCR-03 — Escrow Wire Fraud & Closing Fund Interception Guide

A Complete Handbook and Web Resource for Homebuyers, Sellers, and Real Estate Professionals

Published by Wounded Duck Studios LLC & SCAMREALESTATE.COM
Author: Mark Druckmiller, REALTOR®, Real Estate One (Saline / Washtenaw County, Michigan)

Safe Wiring Protocols & Escrow Wire Fraud Defense

Executive Summary: The $400M Closing Table Threat

Real estate wire fraud is the single most catastrophic cybercrime facing home purchasers today. According to the FBI Internet Crime Complaint Center (IC3), real estate business email compromise (BEC) accounts for hundreds of millions of dollars in annual consumer losses. Unlike credit card theft or unauthorized debit card charges, **wire transfers are instantaneous, final, and virtually irreversible once cleared**.

In a typical escrow wire intercept—such as the recent $185,000 theft from a buyer in Charlotte, North Carolina, and the $128,400 loss from a buyer in Las Vegas—the victim is under contract and preparing to close. Less than 24 to 48 hours before settlement, the buyer receives an email that looks identical to their title company or closing attorney's communication. It references accurate file numbers, purchase prices, and closing dates. It announces a last-minute change to the wiring instructions (e.g., claiming a bank transition, routine escrow audit, or technical maintenance) and directs the buyer to send their down payment and closing funds to a fraudulent account.

Believing the email is legitimate, the buyer wires their life savings. The theft is uncovered only when the buyer sits down at the closing table the next morning and the closing agent asks when the money will be sent. Within minutes, the stolen funds have been laundered across multiple mule accounts or converted into cryptocurrency mixers.

This handbook outlines the exact technical mechanics of real estate wire scams, the four non-negotiable rules of safe wiring, and the immediate emergency response protocol if a fraudulent transfer occurs.

Section 1: Anatomy of an Escrow Wire Interception

Understanding how hackers breach real estate transactions is the key to preventing theft:

1. **Email Compromise (Phishing & Credential Harvesting):** Scammers rarely hack bank databases; instead, they target the email accounts of real estate agents, loan officers, or title settlement staff using targeted phishing emails or credential-stuffing attacks.
2. **Silent Surveillance & Inbox Rules:** Once inside an email account, the attacker does not announce their presence. They set up silent inbox forwarding rules (sending copies of all incoming emails containing words like "wire," "closing," "settlement," or "escrow" to an external server while routing true messages to archive folders).
3. **The Pre-Closing Ambush:** The hacker monitors the transaction until 24 to 72 hours before the scheduled closing. They identify the exact dollar amount needed for settlement and the title company's email thread.
4. **Typosquatted Domain Injection:** The attacker registers a lookalike domain differing by a single character (e.g., changing `@firstamericantitle.com` to `@firstarnericantitle.com` or `@johnsonlawfirm.com` to `@johnson-lawfirm.com`). They reply directly within the existing email thread.
5. **The "Urgent Banking Update" PDF:** The email includes an authentic-looking PDF titled "Updated Wire Transfer Instructions" directing funds to a fraudulent domestic bank account controlled by money mules, warning that settlement will be canceled if funds are not wired immediately.

Section 2: The 4 Non-Negotiable Rules of Safe Wiring

Every homebuyer and real estate professional must memorize and follow these four cardinal rules on every transaction:

Rule 1: Always Conduct an Out-of-Band Phone Verification

- **Never verify wire instructions using the phone number listed in the email itself.** Hackers routinely change the phone number in the signature block of fraudulent emails and answer the phone pretending to be the closing officer.
- **The Protocol:** Look up the title company or closing attorney's phone number on an independent, trusted document received at the very beginning of the transaction (e.g., the original earnest money receipt, your agent's verified contact card, or the company's official public website). Call that independent number, ask for your specific escrow officer by name, and read every digit of the routing number and account number out loud before sending the wire.

Rule 2: Treat ANY Change in Wiring Instructions as Fraud

- **Legitimate title companies almost NEVER change their banking instructions during an active transaction.**
- If you receive any email, phone call, or text message claiming that wire instructions have been updated due to a "bank audit," "system outage," or "new escrow account," **stop immediately**. Treat the message as an active criminal incursion until you have verified it in person or over an independently confirmed phone call.

Rule 3: Verify the Exact Beneficiary Account Name

- When initiating a wire at your bank, ensure the beneficiary name matches the legal name of the title agency or attorney trust account (e.g., "First National Title Agency - Escrow Trust Account"), NOT an individual's personal name or an unfamiliar corporate LLC.
- If your bank teller flags that the routing number corresponds to a regional bank in an unfamiliar state, pause the wire immediately.

Rule 4: Verify Delivery Within 60 Minutes of Transmission

- The moment you leave your bank after initiating the wire, call your escrow officer on their verified phone line. Confirm that the wire was initiated.
- Call back within 60 to 90 minutes to confirm that the funds have physically cleared into the title company's escrow account. Rapid confirmation ensures that if a diversion occurred, you discover it within the critical 24-hour wire recall window.

Section 3: The Homebuyer's Safe Wiring Checklist

Print this checklist and take it with you to your bank:

- ☐ I have obtained the title company's verified phone number from an independent source (not from a wiring instruction email).
- ☐ I have called the escrow officer directly and verified the following details verbally:
  - [ ] Receiving Bank Name
  - [ ] 9-Digit ABA Routing Number
  - [ ] Account Number
  - [ ] Exact Beneficiary Name (Title Company Escrow Trust Account)
  - [ ] Reference / File / Escrow Number
- ☐ I have confirmed that no email was received altering or "updating" the wiring instructions.
- ☐ I have verified that the wire type is a Domestic Federal Wire (not an ACH transfer or peer-to-peer payment app).
- ☐ I have called my escrow officer 60 minutes after wire submission to confirm funds arrived.

Section 4: Emergency Response Protocol — The First 24 Hours

If you discover that you wired funds to a fraudulent account, minutes matter. Execute this 5-step emergency protocol immediately:

1. **Immediate Bank Wire Recall Request (Call Within Minutes):**
   - Contact your sending bank’s wire transfer / fraud department immediately.
   - Request an urgent **SWIFT / Fedwire Recall** on the grounds of criminal wire fraud.
   - Ask your bank to send an urgent administrative notice to the receiving bank's fraud unit requesting an immediate freeze on the recipient account.
2. **Escalate to the FBI Financial Fraud Kill Chain (FFKC):**

- The FBI maintains the Financial Fraud Kill Chain to intercept international and domestic transfers exceeding $50,000 sent within the last 72 hours.
- File an emergency complaint immediately at **ic3.gov**. In the complaint narrative, clearly state: *"REQUEST EMERGENCY FINANCIAL FRAUD KILL CHAIN (FFKC) ASSISTANCE - ACTIVE REAL ESTATE WIRE FRAUD."* Provide sending bank, receiving bank, routing numbers, account numbers, transaction hashes, and exact timestamps.

3. **Contact Local Law Enforcement:**
    - File an official police report with your local police department and the law enforcement agency where the title company is located. Obtain a case incident number.
4. **Contact the Local FBI Field Office & US Secret Service Task Force:**
    - Call the duty agent at your nearest FBI Field Office and the U.S. Secret Service Cyber Fraud Task Force (CFTF). Provide your IC3 complaint number and police report.
5. **Notify the Title Company and Listing Agent:**
    - Alert all parties to audit their email environments, terminate active compromised sessions, and check for unauthorized forwarding rules.

© 2026 Wounded Duck Studios LLC & ScamRealEstate.com. General consumer education only — not legal or financial advice. Questions: irving@woundedduckstudios.com · Call or text 657-305-5210