SCR-14 — Tenant Document Forgery, Fake Paystubs & CPN Screening Guide

A Complete Handbook and Web Resource for Independent Landlords, Property Managers, and Real Estate Professionals

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

Landlord Defense: Conducting Forensic Income Audits, Spotting Doctored Bank PDFs, and Unmasking CPNs

Executive Summary: The Rental Application Fraud Crisis

Application document fraud has surged to crisis levels in residential leasing. According to recent property management industry studies (including national audits by Snappt and the National Multifamily Housing Council), up to 85% of property managers and independent landlords encounter falsified application documents.

In competitive rental markets, unqualified prospective tenants facing prior evictions, poor credit scores, or insufficient income no longer accept rejection. Instead, they turn to widespread online fraud tools:

- **Commercial Paystub Generators:** Websites that generate pixel-perfect W-2s and bi-weekly paystubs complete with corporate logos, earnings breakdowns, and state tax tables for $9.99.
- **Doctored Bank Statement PDFs:** Online graphic editors (Canva, PDFescape, Photoshop) used to alter bank statement balances, change deposit amounts, or fabricate months of regular corporate direct deposits.
- **Credit Profile Numbers (CPNs) / Synthetic Identities:** Fraudsters purchase 9-digit "Credit Privacy Numbers" online—which are actually stolen Social Security numbers belonging to children, incarcerated individuals, or deceased persons—to establish a clean credit profile and hide prior evictions and bankruptcies.

For independent "mom-and-pop" landlords (managing 1 to 4 units) who lack corporate compliance departments, accepting a tenant with falsified documents leads to almost certain default, property damage, and costly eviction proceedings averaging **$6,000 to $12,000+ in legal fees and lost rent**.

This handbook outlines a rigorous 4-Pillar Forensic Document Audit, red flags of manipulated PDFs, how to detect illegal CPNs, and compliant FCRA adverse action procedures.

Section 1: The 4-Pillar Forensic Document Audit

Never approve a residential lease application without executing this four-stage verification protocol:

Pillar 1: Mathematical & Tax Ratio Forensic Verification

Fake paystubs almost always contain mathematical and tax calculation errors:

- **FICA / Social Security Withholding:** Under federal law, the employee Social Security tax rate is strictly **6.2%** of gross wages (up to the annual statutory wage cap). Calculate the exact ratio: `Social Security Tax ÷ Gross Pay`. If the result is not exactly 0.062 (or if the math is rounded incorrectly), the paystub is counterfeit.
- **Medicare Withholding:** The employee Medicare tax rate is strictly **1.45%** of gross wages. Calculate: `Medicare Tax ÷ Gross Pay`. If it does not equal exactly 0.0145, the document was generated by software that guesses deductions.
- **Year-to-Date (YTD) Mathematical Continuity:**
  - Multiply the gross pay per period by the number of pay periods elapsed in the calendar year.
  - Example: If an applicant earns $2,500 bi-weekly and applies on June 30 (13 pay periods elapsed), their YTD Gross Pay should be approximately $32,500. If the paystub displays a YTD gross of $58,000 or $12,000, the numbers were manually fabricated without accounting for pay calendar dates.

Tax Type	Statutory Federal Rate	Verification Formula	Fraud Indicator
Social Security (FICA)	6.20%	`Social Security Tax ÷ Gross Pay`	Any variance from `0.062`
Medicare	1.45%	`Medicare Tax ÷ Gross Pay`	Any variance from `0.0145`
YTD Gross Continuity	Periodic Gross × Elapsed Periods	`Gross Pay × Pay Periods Elapsed`	Variance > 1 pay period equivalent

Pillar 2: PDF Metadata & Digital Artifact Inspection

Scammers typically download legitimate bank statement PDFs or templates and modify them using digital PDF editors:

- **Inspect Document Properties:** In Adobe Acrobat or any PDF reader, click `File > Properties > Description`.
  - Look at **Application** and **PDF Producer**.
  - If a bank statement from Chase or Wells Fargo displays "Canva," "iLovePDF," "PDFescape," "Photoshop," or "Wondershare PDFelement," the document has been tampered with. Legitimate

financial institutions generate statements using enterprise document engines (e.g., "OpenText Exstream" or "Metavante").

- **Font & Kerning Inconsistencies:** Zoom in to 300% on the transaction balance column. Look for subtle misalignments: numbers that float slightly above the baseline, inconsistent font weights, or differing digital resolution between transaction lines.
- **Digital Text Highlighting Test:** Highlight text across the PDF. On authentic statements, text highlights cleanly line-by-line. On doctored PDFs, modified numbers often appear in isolated, floating bounding boxes.

Pillar 3: Bank Statement Cash Flow Reconciliation

Never rely solely on paystubs; cross-reference every paystub directly against official bank statements:

- **Trace the Exact Net Deposit:** If the paystub shows a net take-home pay of $2,143.52 deposited on October 15, verify that the bank statement displays an incoming electronic ACH direct deposit for **exactly $2,143.52** from the claimed employer on that date.
- **Audit Daily Ending Balance Math:** On bank statements, verify that `Previous Daily Balance + Total Deposits - Total Withdrawals = Ending Daily Balance`. Scammers routinely edit deposit lines without updating the running daily balance column, creating mathematical mismatches that expose the forgery.
- **Look for P2P Subsidy Transfers:** Check if the applicant’s deposits are authentic payroll direct deposits or incoming transfers from Cash App, Venmo, or Zelle designed to mimic income.

Pillar 4: Out-of-Band Employer Verification

Never call the employer phone number provided on the tenant application:

- **The Fake Supervisor Trap:** Scammers often list a co-conspirator's cell phone number as their "HR Director" or "Supervisor." When called, the accomplice gives a glowing verbal employment reference.
- **The Out-of-Band Protocol:** Look up the employer's official business registration on your state’s corporate filing portal (e.g., Michigan LARA - Corporations Online Filing System). Verify that the company is active and in good standing. Search the corporate headquarters phone number independently on Google, call the main corporate switchboard, and ask for the Human Resources or Payroll Department.

Section 2: Unmasking Credit Profile Numbers (CPNs)

A **Credit Profile Number (CPN)** is a fraudulent 9-digit number marketed online to consumers with damaged credit as a "legal alternative" to a Social Security number.

The Legal Reality of CPNs:

- **CPNs are completely illegal.** The Social Security Administration does not issue secondary credit numbers.

- CPN sellers purchase or steal unissued Social Security numbers (typically belonging to children born after 2011, elderly individuals, or prisoners) and instruct applicants to use them on credit and rental applications.
- Submitting a CPN on a rental or credit application constitutes **federal false statement fraud and identity theft**.

How to Detect a CPN on a Rental Application:

1. **SSN Issuance Date Inconsistencies:** Run the applicant's 9-digit number through a Social Security verification tool. If a 35-year-old applicant submits an SSN that was issued in 2016, they are using a child's stolen SSN as a CPN.
2. **Thin Credit Files with Sudden High Tradelines:** A CPN profile typically shows a brand-new credit history established within the last 12 to 24 months, but features large "authorized user" credit card tradelines with zero historical utility or installment accounts.
3. **Mismatched Public Record Addresses:** Credit bureau public records checks show zero historical residential addresses or motor vehicle registrations linked to that number prior to the last two years.

Section 3: FCRA-Compliant Adverse Action Protocol

When rejecting an applicant who submitted fraudulent or unverifiable documents, you must comply with the federal **Fair Credit Reporting Act (FCRA)** and **Fair Housing Act**:

1. **Document the Factual Deficiency:** Base the adverse action on objective, non-discriminatory criteria outlined in your written Tenant Selection Policy (e.g., *"Inability to verify employment through independent corporate records"* or *"Discrepancies in submitted financial documentation"*).
2. **Issue a Formal Adverse Action Notice:** If credit bureau reports were utilized in any part of the screening process, send a written Adverse Action Notice within statutory deadlines including:
    - The name, address, and toll-free telephone number of the consumer reporting agency (CRA) used.
    - A statement that the CRA did not make the decision and cannot explain why it was made.
    - Notice of the applicant's right to obtain a free copy of their credit report within 60 days and dispute any inaccurate information.
3. **Retain All Screening Records:** Archive the application, submitted documents, metadata analysis, and adverse action notice for a minimum of three years to defend against potential fair housing claims.

© 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