Shufti

Combating Proof Of Address Fraud

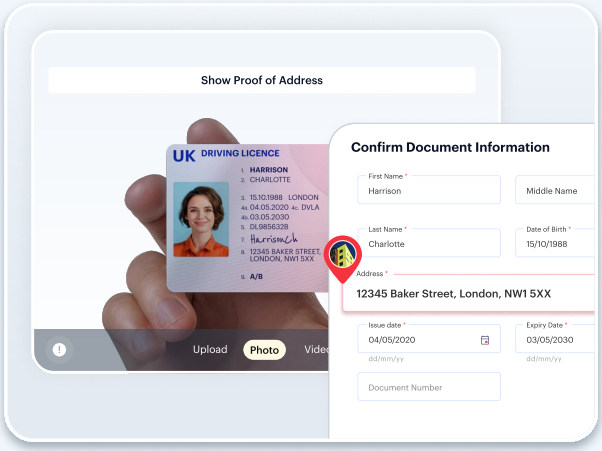
PCI DSS · SOC2 · GDPR · QG GDPR · ISO 27001: 2013 · CE+ · iBeta Level 1 · iBeta Level 2 · KJM Verification age · CCPA

Multi-Layered Forensic Analysis For Bank Statements, Salary Slips, Utility Bills, And Address Documents

Proof of Address (PoA) verification is a critical component of customer onboarding across financial services, fintech, telecom, and regulated industries. However, address document fraud has evolved rapidly in recent years, making traditional manual review and simple document checks increasingly ineffective.

Fraudsters today use a wide range of techniques to manipulate or fabricate address documents, from simple edits to AI-generated templates.

Shufti's Address Verification solution is designed to detect these threats through advanced AI analysis, document forensics, and multi-layered fraud detection.



Shufti provides both:

Document-Based Address Verification | **Docless eIDV Address Verification**

It gives organizations the flexibility to choose the most appropriate verification method for each user and use case.

This document illustrates common address fraud techniques and how Shufti's technology identifies and prevents them.

In addition to document-based verification, Shufti also provides docless eIDV Address Verification, giving organizations the flexibility to choose the most appropriate verification method for each user and use case.

Understanding Address Document Fraud

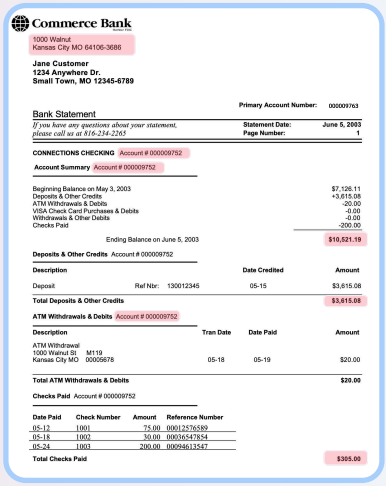
Proof of Address fraud can appear in many different formats and submission methods. Fraudsters frequently manipulate utility bills, bank statements, rent agreements, and other address documents to bypass onboarding checks.

Common Address Fraud Techniques

PDF Template Editing

A utility bill or bank statement template is purchased online and modified in a PDF editor. Names, addresses, amounts, and dates are changed while logos, watermarks, and layout remain authentic.

Edits leave traces in file metadata and internal structure, but are invisible to the human eye.



Commerce Bank

1000 Walnut
Kansas City MO 64106-3686

Jane Customer
1234 Anywhere Dr.
Small Town, MO 12345-6789

Primary Account Number: 000009763

Bank Statement

If you have any questions about your statement, please call us at 816-234-2265

Statement Date: June 5, 2003
Page Number: 1

CONNECTIONS CHECKING Account # 000009752

Account Summary Account # 000009752

Beginning Balance on May 3, 2003	$7,126.11
Deposits & Other Credits	+3,615.08
ATM Withdrawals & Debits	-20.00
VISA Check Card Purchases & Debits	-0.00
Withdrawals & Other Debits	-0.00
Checks Paid	-200.00
Ending Balance on June 5, 2003	$10,521.19

Deposits & Other Credits Account # 000009752

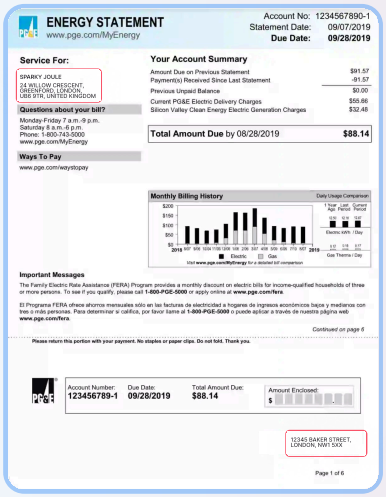
Description		Date Credited	Amount
Deposit	Ref Nbr: 130012345	05-15	$3,615.08
Total Deposits & Other Credits			$3,615.08

ATM Withdrawals & Debits Account # 000009752

Description	Tran Date	Date Paid	Amount
ATM Withdrawal 1000 Walnut St M119 Kansas City MO 0009678	05-18	05-19	$20.00
Total ATM Withdrawals & Debits			$20.00

Checks Paid Account # 000009752

Date Paid	Check Number	Amount	Reference Number
05-12	1001	75.00	00012576589
05-18	1002	50.00	00036547854
05-24	1003	200.00	00094613547
Total Checks Paid			$305.00



ENERGY STATEMENT
www.pge.com/MyEnergy

Account No: 1234567890-1
Statement Date: 09/07/2019
Due Date: 09/28/2019

Service For:

SPARKY JOULE
14 WILLOW CRESCENT,
GREENFORD, LONDON,
UB5 6TR, UNITED KINGDOM

Your Account Summary

Amount Due on Previous Statement	$91.57
Payment(s) Received Since Last Statement	-91.57
Previous Unpaid Balance	$0.00
Current PG&E Electric Delivery Charges	$55.66
Silicon Valley Clean Energy Electric Generation Charges	$32.48
Total Amount Due by 08/28/2019	**$88.14**

Questions about your bill?
Monday-Friday 7 a.m.-9 p.m.
Saturday 8 a.m.-6 p.m.
Phone: 1-800-743-5000
www.pge.com/MyEnergy

Ways To Pay
www.pge.com/waystopay

Monthly Billing History

Important Messages

Account Number: 123456789-1 | Due Date: 09/28/2019 | Total Amount Due: $88.14 | Amount Enclosed: $

12345 BAKER STREET,
LONDON, NW1 5XX

Page 1 of 6

Screenshot Manipulation

A bank statement or utility portal is opened in a browser. Values are modified using browser developer tools. The result is screenshotted, producing a pixel-perfect fake with no compression artifacts, no metadata anomalies, and no structural traces. Traditional document analysis cannot catch this.

Photograph or Scan & Resubmit

A previously used or fraudulent physical document is photographed or scanned and resubmitted as a new copy. The scan introduces noise that masks editing artifacts, making it harder to detect tampering through metadata analysis alone.

HSBC UK

Your Statement

Mr Toby Grant
Flat 2
27 Argyll Road
London
W8 7DA

Account Summary

Opening Balance	0.57
Payments In	3,142.37
Payments Out	1,003.10
Closing Balance	2,139.27
Arranged Overdraft Limit	0.00

International Bank Account Number
GB24HBUK40891338292 63
Branch Identifier Code
HBUKGB4195W

25 November to 2 December 2023

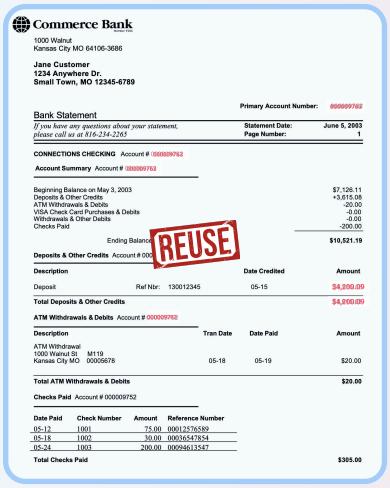
Account name
Mr Toby Grant

Sortcode 40-25-01 | Account Number 74329263 | Sheet Number 16

Your Bank Account details

Date	Payment type and details	Paid out	Paid in	Balance
24 Nov 23	BALANCE BROUGHT FORWARD			0.57
25 Nov 23	CR Transfer		2,212.14	2,212.71
26 Nov 23	BP Telephone Bill Payment MASTERCARD	60.00		152.71
27 Nov 23	BP DHL delivery services	30.50		122.71
28 Dec 23	CR Cheque Deposit		425.23	
29 Nov 23	CR Jessica George		500.00	
	BP Shell 2-4 NEW CROSS ROAD	202.34		27.76
	BP Pizza Union Hoxton	15.13		27.76
30 Dec 23	BP Uber	28.90		1.53
01 Dec 23	BP British Gas Payment MASTERCARD	659.23		17.27
02 Dec 23	BP Costa Cofee	7.00		10.27
	BALANCE CARRIED FORWARD			2,139.27

Reused or Stolen Documents



Commerce Bank

1000 Walnut
Kansas City MO 64106-3686

Jane Customer
1234 Anywhere Dr.
Small Town, MO 12345-6789

Primary Account Number:

Bank Statement

If you have any questions about your statement, please call us at 816-234-2265

Statement Date: June 5, 2003
Page Number: 1

CONNECTIONS CHECKING Account #

Account Summary Account #

Beginning Balance on May 3, 2003	$7,126.11
Deposits & Other Credits	+3,615.08
ATM Withdrawals & Debits	-20.00
VISA Check Card Purchases & Debits	-0.00
Withdrawals & Other Debits	-0.00
Checks Paid	-200.00
Ending Balance	$10,521.19

REUSE

Deposits & Other Credits Account #

Description		Date Credited	Amount
Deposit	Ref Nbr: 130012345	05-15	$4,200.09
Total Deposits & Other Credits			$4,200.09

ATM Withdrawals & Debits Account #

Description	Tran Date	Date Paid	Amount
ATM Withdrawal 1000 Walnut St M119 Kansas City MO 00005678	05-18	05-19	$20.00
Total ATM Withdrawals & Debits			$20.00

Checks Paid Account # 000009752

Date Paid	Check Number	Amount	Reference Number
05-12	1001	75.00	00012576589
05-18	1002	30.00	00036547854
05-24	1003	200.00	00094613547
Total Checks Paid			$305.00

Using found, stolen, or previously verified documents in a new application without authorization. The document itself may be entirely genuine, the fraud lies in the identity mismatch between the document holder and the applicant.

Because these documents often look legitimate to the human eye, detecting fraud requires analysis beyond simple visual inspection.

Why This Matters for Bank Statements & Salary Slips

Bank statements and salary slips are the most frequently targeted PoA documents because they serve a dual purpose by verifying both **Address** **Financial Standing**

Bank statements and salary slips are the most frequently targeted PoA documents because A single forged bank statement can simultaneously satisfy PoA requirements and inflate perceived income, making them the highest-value target for organized fraud operations. Salary slips carry similar dual-use risk, with the added complexity of employer verification requirements.

Shufti's Multi-Layered Approach To Address Verification Fraud Defense

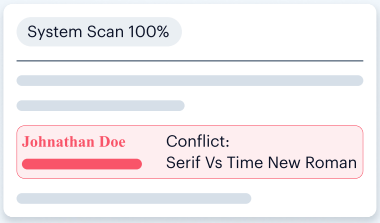
Shufti's Address Verification solution is built around a **defense-in-depth approach**. Rather than relying on a single detection technique, multiple independent verification layers work together to identify manipulation and fraud signals. Every document uploaded to Shufti passes through several independent analysis layers. These layers execute in parallel where possible, and their outputs are aggregated into a composite risk score.

Each layer analyzes different aspects of the document, including:

- **Document structure**
- **Font and layout consistency**
- **Pixel-level image analysis**
- **Metadata and edit history**
- **Field-level comparisons**
- **Cross-submission document matching**

This layered approach significantly increases the difficulty and cost for fraudsters attempting to bypass verification systems.

Layer 1



Font Consistency Analysis

Examines whether the typography used across a document is consistent. Fraudulent edits often introduce subtle font inconsistencies when fields such as names or addresses are replaced.

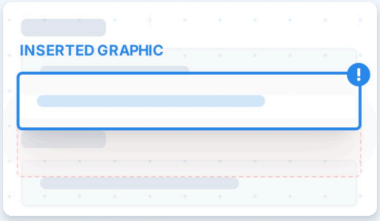
How Shufti Applies This

Shufti analyzes the font family, weight, and rendering characteristics of text elements throughout the document. If specific fields differ from the document's baseline typography, the system flags the inconsistency.

Detection Example

A fraudster removes a customer name from a utility bill and retypes it using a different font. Although visually convincing, the system detects that the replacement text uses a different font family than the rest of the document and flags the modification as suspicious.

Layer 2



Overlay & Insert Detection

Identifies cases where visual elements such as images or graphics have been inserted to replace or hide original text fields.

How Shufti Applies This

Shufti analyzes document structure to determine whether objects have been added to areas that should contain native text elements. Inserted overlays often indicate manipulated fields.

Detection Example

A fraudster overlays an image containing new numbers over the original balance on a utility bill. While the change appears seamless, Shufti detects that an image has been inserted into a text-only area and identifies that the document was edited after its original creation.

Layer 3

Document Edit History Detection

Detects whether a document has been edited multiple times during the manipulation process.

How Shufti Applies This

By analyzing document structure and revision patterns, Shufti identifies whether multiple editing sessions have occurred, which is a strong indicator of manipulation.

Detection Example

A fraudster edits a utility bill in several steps; first changing the name, then modifying the billing amount, and finally replacing the address. Shufti detects multiple separate edits and flags the document as high risk.

Layer 4

AI-Based Image Manipulation Detection

Identifies visual manipulation in documents submitted as images, photographs, scans, or screenshots.

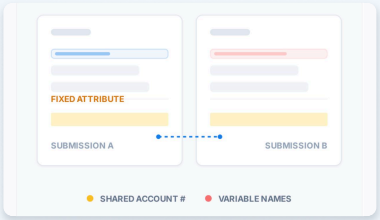
How Shufti Applies This

Shufti applies AI-driven pixel-level analysis to detect inconsistencies in image patterns. The system generates a manipulation heatmap highlighting regions that may have been altered.

Detection Example

A scanned document shows signs of editing in the name and billing fields. The AI analysis highlights these areas as having a high probability of manipulation, even though the changes are not visible to the human eye.

Layer 5



Cross-Submission Document Intelligence

Detects when the same document is reused across multiple identities.

How Shufti Applies This

The system compares extracted document data against previously submitted documents to identify reused templates or identical document structures with modified personal details.

Detection Example

A utility bill previously submitted under one name appears again with a different identity. While the personal details differ, key document attributes such as account number, issuer, and reference values match an earlier submission, indicating document reuse.

Layer 6

AI-Generated Document Pattern Detection

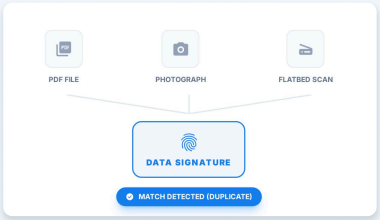
Identifies batches of documents generated from a single template using AI tools.

How Shufti Applies This

The system analyzes structural similarities across documents, including layout patterns, font rendering, color profiles, and watermark structures.

Detection Example

Multiple utility bills are submitted with different names and addresses but share identical layout and visual characteristics. Shufti identifies the shared template and flags the submissions as likely AI-generated variations.



Layer 7

Cross-Format Document Reuse Detection

Detects when the same document is submitted in different formats to bypass detection.

How Shufti Applies This

Shufti extracts structured data from documents regardless of format — whether submitted as a PDF, photograph, or scan — and compares this information across submissions.

Detection Example

The same bank statement is submitted three times: once as a PDF, once as a photograph, and once as a scanned image. Although visually different, the extracted data matches across all three submissions, allowing the system to identify the document as a duplicate.

Benefits for Compliance and Fraud Teams

Shufti Address Verification is designed to help organizations strengthen onboarding security while maintaining a smooth user experience.

Key Benefits

Detect Sophisticated Document Fraud

Advanced document analysis detects manipulation techniques such as template editing, overlay attacks, and AI-generated documents that may bypass traditional checks.

Reduce Manual Review Workload

Automated fraud detection reduces reliance on manual document inspection, allowing compliance teams to focus on higher-risk cases.

Improve Regulatory Compliance

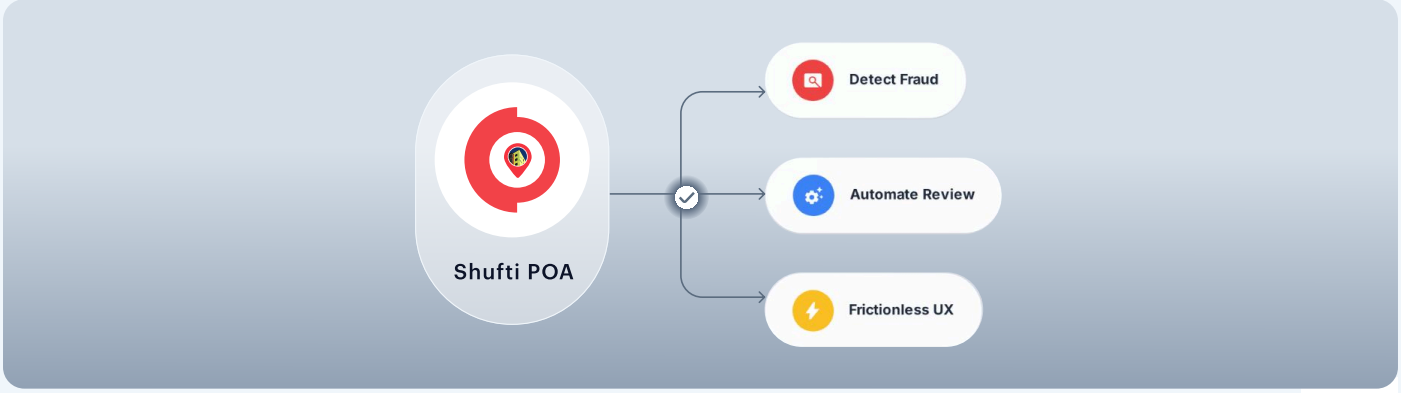
Reliable address verification supports regulatory obligations such as KYC, AML, and customer due diligence requirements.

Identify Fraud Patterns Across Submissions

Cross-document intelligence allows organizations to detect when the same document template is reused across multiple identities or accounts.

Maintain a Frictionless Customer Experience

Verification processes are designed to detect fraud signals without introducing unnecessary friction for legitimate users.



Solution Capabilities

Shufti Address Verification combines AI-powered document analysis with global coverage and scalable verification infrastructure.

Multi-layered fraud detection

Multiple independent analysis layers evaluate document structure, visual integrity, and cross-submission patterns.

Global document coverage

Support for broad document types across 230+ countries and territories.

Fast verification times

Verification results are typically delivered in under 30 seconds, enabling seamless onboarding experiences.

Cross-document intelligence

Detects reused documents and fraud patterns across multiple submissions.

Flexible integration

Available through APIs and SDKs that integrate easily into existing onboarding workflows.

Strengthen Your Address Verification Strategy

Address fraud is evolving rapidly, from simple document edits to AI-generated forgeries produced at scale.

Organizations need verification systems capable of detecting manipulation patterns that are invisible to the human eye.

Shufti Address Verification combines **AI-powered document analysis**, **cross-document intelligence**, and **multi-layered fraud detection** to protect onboarding pipelines while maintaining a seamless customer experience.

In addition to document-based verification, Shufti also offers docless eIDV address verification, enabling organizations to verify addresses through trusted data sources without requiring users to upload documents. This flexibility allows businesses to tailor verification flows to their specific risk models, applying document checks where necessary while enabling lower-friction verification for trusted users.

By combining both approaches, organizations can build onboarding journeys that are secure, compliant, and optimized for conversion.

Contact Sales

See how Shufti Address Verification can strengthen your fraud defenses.

Book a Demo

SALES@SHUFTI.COM WWW.SHUFTI.COM