An Analysis of Current Affordable Care Act Fraud Vulnerabilities Removed by Health Savings Account Identity Verification

A Comparative Assessment of Identity Verification Standards, Enforcement Mechanisms, with Legislative and Policy Recommendations

January 2026

Prepared by
The HSA Coalition

Table of Contents

Executive Summary 4

1. GAO Undercover Investigation of ACA Marketplace Controls 5

2. ACA Marketplace Enrollment Process and Verification Standards 7

3. ACA Marketplace Fraud Enforcement Framework 9

4. Health Savings Account Opening Requirements 13

5. Comparative Analysis: Verification Standards 16

6. Illustrative Analysis: HSA-Based Subsidy Model 19

7. Policy Implications and Recommendations 22

8. Summary of Findings 26

9. Conclusion 27

Appendix: Regulatory Citations 29

Executive Summary

This report analyzes the contrast between identity verification requirements for Affordable Care Act (ACA) marketplace enrollment and Health Savings Account (HSA) opening procedures, and presents a comprehensive policy framework for addressing documented fraud vulnerabilities. The analysis is particularly relevant in light of the Government Accountability Office (GAO) undercover investigations, which found that 96% of fictitious test applications were approved in 2023, and 90% of fictitious applicants submitted in 2024-2025 remain actively covered with subsidies exceeding $10,000 per month.

The findings reveal a significant disparity in fraud prevention mechanisms:

- ACA marketplace enrollment relies primarily on self-attestation-based verification with limited real-time identity validation, allowing provisional enrollment before verification is complete
- HSA account opening requires stringent Know Your Customer (KYC), OFAC screening, and Bank Secrecy Act/USA PATRIOT Act compliance before account activation
- Criminal prosecution of ACA enrollment fraud has been minimal—fewer than 10 federal cases through 2025 despite 275,000+ consumer complaints in 2024 and 160,000 likely unauthorized broker changes identified by GAO
- The Health Care Fraud and Abuse Control (HCFAC) program is statutorily limited to Medicare and Medicaid, leaving no dedicated federal enforcement funding for ACA marketplace fraud
- The HEAT Strike Force has charged over 5,800 defendants in Medicare/Medicaid fraud since 2007; no comparable enforcement mechanism exists for the ACA marketplace

Primary Recommendation: Three-Pillar HSA Subsidy Framework

This analysis recommends Congress authorize an integrated HSA-Based Subsidy Delivery Model built on three pillars: (1) Uniform Identity Standards requiring CIP compliance equivalent to 31 CFR § 1020.220; (2) Automated Eligibility Bridging through real-time API verification to eliminate provisional enrollment exploitation; and (3) Public-Private Safety Net Accounts to ensure healthcare access for unbanked populations while maintaining verification integrity.

Additional Recommendations:

- Strengthen income verification through real-time payroll data access and tiered verification with hard-stop documentation for deviations exceeding 10% from IRS records

- Expand HCFAC jurisdiction by amending 42 U.S.C. § 1320a-7c to fund ACA marketplace fraud investigations
- Require mandatory disclosure of CMS findings for broker suspensions exceeding 30 days
- Establish a dedicated Marketplace Strike Force modeled after the successful HEAT program

This analysis concludes that adopting banking-level verification standards, combined with income verification reforms and expanded enforcement jurisdiction, would substantially reduce vulnerability to fraudulent enrollment while preserving access to healthcare subsidies for legitimately eligible Americans.

1. GAO Undercover Investigation of ACA Marketplace Controls

1.1 Overview of the Investigation

In 2023, the Government Accountability Office conducted an undercover investigation to test the effectiveness of fraud prevention controls in the ACA marketplace enrollment process. The investigation involved submitting 24 fictitious applications designed to test various aspects of the verification system.

1.2 Key Test Results

Test Application Success Rate: The GAO's undercover testing successfully enrolled 23 out of 24 fictitious applicants (95.8% test success rate). While these results demonstrate vulnerabilities in the system's ability to detect fraudulent applications under controlled testing conditions, they should not be interpreted as measuring overall fraud rates in the actual marketplace, which remain unknown.

Types of Fraudulent Applications That Succeeded:

- Fabricated Social Security Numbers that failed standard validation
- Fictitious identities with no credit history or verifiable records
- Income discrepancies that should have triggered verification
- Invalid documentation that bypassed document authentication systems

1.3 Financial Impact

The successful test enrollments resulted in federal subsidies being improperly awarded in the GAO's controlled investigation. The testing revealed that the marketplace systems processed applications and initiated subsidy payments without adequate verification of:

- Identity authenticity
- Income eligibility
- Citizenship or lawful presence
- Document authenticity

The investigation demonstrated that federal subsidies totaling thousands of dollars per fictitious application were committed before any verification failures were detected, if they were detected at all.

1.4 Systemic Vulnerabilities Identified

Reliance on Self-Attestation: Within its current regulatory framework, the ACA marketplace relies heavily on applicant self-attestation rather than real-time verification of claimed information.

Limited Data Cross-Checking: Systems had difficulty adequately cross-referencing applicant information with authoritative databases, including the Social Security Administration, the IRS, and Department of Homeland Security records.

Document Verification Gaps: The documentation submitted by applicants was not subjected to authentication protocols sufficient to detect fabricated or altered documents in banking contexts.

Delayed Post-Enrollment Verification: When verification processes were triggered, they occurred after subsidies had already been committed or paid, creating opportunities for fraudulent enrollment to succeed before detection.

2. ACA Marketplace Enrollment Process and Verification Standards

2.1 Application Process Overview

The ACA marketplace enrollment process, operating under its statutory and regulatory framework, is designed to provide accessible healthcare coverage to eligible individuals. The application can be completed online, by phone, by mail, or with in-person assistance. The process follows these general steps:

- Account Creation: Applicants create an account on Healthcare.gov or a state-based marketplace with basic identity information (email address and password)
- Information Entry: Applicants provide personal information including name, date of birth, Social Security Number, address, income, and household composition
- Eligibility Determination: The system processes the application and determines eligibility for coverage and financial assistance
- Plan Selection: Applicants choose from available health plans
- Enrollment Completion: Coverage begins after the first premium payment (if applicable)

2.2 Identity Verification Methods

Electronic Data Verification: Within current regulatory requirements, the marketplace attempts to verify identity electronically by checking information against federal data sources including:

- Social Security Administration (SSA) records
- Department of Homeland Security (DHS) citizenship/immigration status
- Internal Revenue Service (IRS) income data
- CMS records for existing Medicare, Medicaid, and CHIP enrollment
- Other existing health coverage information

Verification Framework Differences: However, the verification processes permitted under ACA marketplace regulations differ from banking-sector requirements, with verification sometimes being incomplete, delayed, or reliant on self-attestation when electronic verification is unavailable.

2.3 Self-Attestation and Document Submission

When electronic verification is unsuccessful or unavailable, current ACA marketplace procedures allow applicants to proceed based on self-attestation with a requirement to submit supporting documentation. This regulatory approach creates certain vulnerabilities:

- Provisional Enrollment: Applicants can be provisionally enrolled with subsidies while documentation is pending
- Extended Timeframes: Applicants may have 90 days or more to submit documentation, during which benefits continue

- Document Authentication Standards: Submitted documents are reviewed by human evaluators using different protocols than the sophisticated fraud detection technology employed by financial institutions
- Variable Follow-up: Follow-up on missing or questionable documentation varies by marketplace and circumstances

2.4 Income Verification Challenges

Income verification presents particular challenges because subsidy eligibility is based on projected annual income rather than historical data:

- Projected Income: Applicants self-report expected income for the coverage year, which cannot be verified in real-time
- IRS Data Lag: IRS data is typically 1-2 years behind, making it difficult to validate current income claims
- Verification Triggers: Large discrepancies between IRS data and reported income may not consistently trigger verification requirements under current procedures
- Reconciliation After-the-Fact: Income is reconciled when filing taxes the following year, long after subsidies have been paid

2.5 Fraud Detection Technology Comparison

The ACA marketplace operates under a different technological framework than financial institutions:

- No OFAC Screening: Current marketplace procedures do not include screening against Office of Foreign Assets Control sanctions lists
- No Credit Bureau Validation: Marketplace regulations do not require verification of identity through credit reporting agencies
- Limited Biometric Verification: No fingerprint, facial recognition, or other biometric authentication in current procedures
- Pattern Analysis: Different approach to use of artificial intelligence or machine learning for detecting fraudulent patterns
- No Customer Identification Program Requirement: Unlike banks, marketplaces are not required under current law to implement formal Customer Identification Programs (CIP) as defined in banking regulations

3. ACA Marketplace Fraud Enforcement Framework

Understanding the enforcement framework for ACA marketplace fraud is essential to evaluating the comparative effectiveness of fraud prevention mechanisms. While the ACA includes provisions for addressing fraud, the enforcement structure differs fundamentally from the banking sector's comprehensive regulatory regime.

3.1 Statutory Authority and Responsible Agencies

The Affordable Care Act grants the Secretary of the Department of Health and Human Services (HHS) authority to determine appropriate activities to reduce fraud and abuse in the administration of Marketplaces and to investigate Marketplace activity. The HHS Secretary oversees these functions through several agencies:

- Centers for Medicare and Medicaid Services (CMS): Primary administrative oversight of the federally-facilitated marketplace (Healthcare.gov)
- Center for Consumer Information and Insurance Oversight (CCIIO): Oversees marketplace operations and agent/broker compliance
- Center for Program Integrity (CPI): Focuses on program integrity across CMS programs
- HHS Office of Inspector General (OIG): Conducts audits and investigations, though with jurisdictional limitations discussed below
- Department of Justice (DOJ): Litigates civil and criminal actions involving alleged health care fraud

3.2 Civil Penalties Under Section 1411

Section 1411 of the ACA establishes civil penalty authority for marketplace fraud. The penalties are structured as follows:

Violation Type	Standard	Maximum Penalty
Negligent provision of false information	Failure to make reasonable attempt to provide accurate information	Up to $25,000 per application
Knowing and willful provision of false information	Intentional provision of information known to be false or fraudulent	Up to $250,000
Improper use or disclosure of information	Knowing and willful violation of Section 1411(g)	Up to $25,000 per use/disclosure

Importantly, no penalty may be imposed for negligent violations if HHS determines there was reasonable cause for the failure and the person acted in good faith.

3.3 False Claims Act Application

The ACA specifies that payments made in connection with Marketplaces are subject to the False Claims Act (FCA) if these payments include federal funds. The FCA provides for:

- Civil penalties of $13,946 to $27,894 per false claim (adjusted annually for inflation)
- Treble damages (three times the amount of damages sustained by the government)
- Qui tam provisions allowing private individuals to file suits on behalf of the government and receive a portion of recovered funds
- The ACA increased penalties available for False Claims Act violations

3.4 Critical Limitation: HCFAC Jurisdictional Gap

A significant structural limitation in ACA marketplace fraud enforcement is the jurisdictional scope of the Health Care Fraud and Abuse Control (HCFAC) program. HCFAC is the primary federal mechanism for coordinating healthcare fraud enforcement and has demonstrated substantial returns on investment for Medicare and Medicaid fraud prevention.

Key Limitation: Under current law, OIG can only use HCFAC funding for program integrity activities related to Medicare and Medicaid. The ACA Marketplace and related programs such as the Advanced Premium Tax Credit (APTC) program are excluded from HCFAC's statutory jurisdiction.

This jurisdictional gap has several significant implications:

- No dedicated federal fraud enforcement funding stream for ACA marketplace fraud investigations
- The highly effective HEAT (Health Care Fraud Prevention and Enforcement Action Team) Strike Force teams cannot be deployed for marketplace fraud
- OIG audit and investigative resources cannot be funded through HCFAC for marketplace-specific fraud schemes
- The proven fraud prevention infrastructure that delivers $4-8 return on investment in Medicare/Medicaid is unavailable for the ACA marketplace

3.5 Agent and Broker Oversight

CMS has developed a framework to regulate agents and brokers who assist consumers with marketplace enrollment. This framework has evolved in response to widespread reports of fraudulent agent and broker activity:

- CMS can suspend and terminate marketplace agreements with agents and brokers engaged in fraudulent or abusive conduct
- Between June and October 2024, CMS suspended 850 agents and brokers for suspected fraudulent activity related to unauthorized enrollments
- CMS received over 73,000 consumer complaints involving agent/broker misconduct in FY 2023 alone

- In the first three months of 2024, CMS received approximately 40,000 complaints of unauthorized plan switches and 50,000 complaints of unauthorized enrollments

3.6 Enforcement Comparison: ACA vs. Banking Sector

The following table highlights the structural differences between ACA marketplace fraud enforcement and the banking sector's regulatory framework:

Enforcement Element	ACA Marketplace	Banking Sector (HSA)
Dedicated Fraud Enforcement Funding	No dedicated funding stream; HCFAC excluded by statute	HCFAC funding available; dedicated compliance budgets
Maximum Civil Penalty (Individual Fraud)	Up to $250,000	Up to $25,000 per violation (BSA); up to twice transaction amount (OFAC)
Criminal Penalties	Available through DOJ prosecution	Up to $500,000 and 10 years imprisonment
Criminal Prosecutions (Historical)	Fewer than 10 federal cases through 2025 despite 275,000+ complaints in 2024	HCFAC Strike Force: 5,800+ defendants charged since 2007
Regulatory Examinations	Limited; no routine compliance examinations	Regular examinations by OCC, FDIC, Federal Reserve, FinCEN
License/Charter Revocation	N/A - marketplace is government-operated	Banking charter revocation possible
Dedicated Fraud Detection Resources	CPI staff; limited specialized resources	Dedicated compliance officers; fraud analytics teams
Return on Investment Data	Not tracked for marketplace-specific enforcement	Medicare enforcement: $4-8 return per $1 spent

3.7 Criminal Prosecution Record

Despite the scale of documented fraud vulnerabilities and hundreds of thousands of consumer complaints, criminal prosecutions for ACA enrollment fraud have been extremely limited. The following represents the known federal prosecution activity as of late 2025:

Case/Action	Status (as of late 2025)	Alleged Fraud Amount
Lloyd & Strong (FL/TX)	Convicted November 2025	$233 million (at least $180 million paid)
Dafud Iza (FL)	Guilty plea April 2025	$133.9 million
Simple Health Plans (FL)	Convicted February 2024	$195 million (civil judgment)
CMS Administrative Suspensions	850 brokers suspended June-Oct 2024; all reinstated by May 2025	N/A

Key Observations on Prosecution Activity:

- Total known federal criminal prosecutions for ACA enrollment fraud: Fewer than 10 cases through 2025, despite 275,000+ consumer complaints in 2024 alone
- Combined alleged fraud in known prosecutions: Approximately $562 million across three major cases
- No criminal penalties have been imposed under Section 1411(h) civil monetary penalty authority as of late 2025
- The 850 brokers suspended by CMS in 2024 were all reinstated by May 2025 without public disclosure of investigatory findings
- GAO identified 160,000 likely unauthorized broker changes in 2024 alone, yet criminal referrals remain minimal
- Contrast with HCFAC-funded Medicare/Medicaid fraud: The Strike Force program has charged over 5,800 defendants since 2007, securing billions in recoveries

The disparity between the volume of documented fraud indicators and the minimal prosecution activity underscores the structural enforcement limitations facing ACA marketplace oversight, including the exclusion of marketplace fraud from HCFAC funding and dedicated fraud investigation resources.

3.8 State-Level Enforcement

States serve as the primary regulators of private insurance coverage available in the Marketplaces, and 20 states operate their own marketplace. Each state has parallel authority to oversee program integrity and address fraud, including:

- State insurance commissioner oversight of agents and brokers
- State false claims act provisions (where enacted)
- State-level consumer protection enforcement
- Coordination with federal authorities on cross-jurisdictional matters

However, the effectiveness of state-level enforcement varies significantly based on state resources, statutory authority, and enforcement priorities.

4. Health Savings Account Opening Requirements

4.1 Regulatory Framework Overview

Health Savings Accounts are deposit accounts offered by financial institutions, which means they are subject to the full spectrum of banking regulations. These requirements are federal mandates with severe penalties for non-compliance.

4.2 Bank Secrecy Act Requirements

The Bank Secrecy Act (BSA) of 1970, as amended by the USA PATRIOT Act, establishes comprehensive requirements for customer identification and verification:

- Customer Identification Program (CIP): Financial institutions must implement a written CIP that includes risk-based procedures for verifying customer identities
- Minimum Information Requirements: Institutions must obtain at minimum: name, date of birth, address, and identification number (typically SSN for U.S. citizens)
- Identity Verification Methods: Institutions must verify identity through documents, non-documentary methods, or a combination
- Record Retention: All identifying information and verification documentation must be retained for five years after account closure

4.3 Know Your Customer (KYC) Protocols

KYC requirements go beyond basic identity verification to establish a comprehensive understanding of the customer:

- Multi-Factor Authentication: Verification through multiple independent sources and methods
- Documentary Verification: Review of government-issued identification documents (driver's license, passport) with authentication checks
- Non-Documentary Verification: Cross-referencing with credit bureaus, utility records, employment verification, or other independent data sources
- Risk-Based Enhanced Due Diligence: Additional verification for higher-risk customers or unusual account features
- Beneficial Ownership: For accounts opened by legal entities, identification of individuals who own or control the entity

4.4 OFAC Screening Requirements

The Office of Foreign Assets Control (OFAC) of the U.S. Department of Treasury maintains lists of individuals and entities with whom U.S. persons and institutions are prohibited from doing business. Financial institutions must:

- Initial Screening: Screen all new customers against OFAC's Specially Designated Nationals (SDN) list and other sanctions lists
- Ongoing Monitoring: Continuously monitor existing customers against updated OFAC lists

- Interdiction: Block or reject transactions involving sanctioned parties
- Reporting: Report blocked transactions to OFAC within specified timeframes
- False Positive Management: Implement procedures to investigate and clear false positive matches

4.5 USA PATRIOT Act Section 326 Compliance

Section 326 of the USA PATRIOT Act specifically mandates customer identification procedures for financial institutions:

- Mandatory CIP: Every financial institution must have a written Customer Identification Program
- Identity Verification Standard: Must enable the institution to form a reasonable belief that it knows the true identity of each customer
- Certification: Institutions must certify to regulatory authorities that they have implemented required procedures
- Notice to Customers: Customers must be notified that information is being collected for identity verification purposes
- Comparison with Government Lists: Within a reasonable time after account opening, verify customer identity against government-provided lists of suspected terrorists

4.6 Technology-Enabled Verification

Many HSA providers utilize sophisticated technology for identity verification, though specific implementations vary by institution:

- Knowledge-Based Authentication (KBA): Out-of-wallet questions based on the applicant's credit history that only the true individual could answer
- Device Fingerprinting: Analysis of device characteristics to detect suspicious patterns (increasingly common among larger institutions)
- Geolocation Verification: Comparison of stated address with device location data where available
- Document Authentication: Optical character recognition and security feature detection to validate ID documents (adoption varies by institution size and resources)
- Biometric Verification: Facial recognition comparing selfies to government-issued ID photos (increasingly adopted by larger financial institutions, though not yet universal)
- Behavioral Analytics: Analysis of application completion patterns to detect bot activity or fraudulent behavior (more common among institutions with advanced fraud analytics capabilities)

4.7 Penalties for Non-Compliance

Financial institutions face severe consequences for failing to comply with identity verification requirements:

- Civil Penalties: Up to $25,000 per violation for BSA violations; up to twice the transaction amount for OFAC violations

- Criminal Penalties: Fines up to $500,000 and imprisonment up to 10 years for willful violations
- Regulatory Actions: Cease and desist orders, removal of officers/directors, prohibition from banking industry
- Reputational Damage: Public enforcement actions and loss of customer confidence
- License Revocation: Loss of banking charter in extreme cases

These substantial penalties create strong institutional incentives for rigorous compliance, which differs from the enforcement structure applicable to ACA marketplaces.

5. Comparative Analysis: Verification Standards

The following analysis compares identity verification, fraud prevention mechanisms, and enforcement structures between ACA marketplace enrollment and HSA account opening. It is important to note that each system operates under its own distinct regulatory framework with different policy objectives and compliance requirements.

Verification Element	ACA Marketplace	HSA Account Opening
Identity Verification Method	Primary reliance on self-attestation with electronic verification against SSA/DHS databases where available	Multi-factor authentication including documentary verification, non-documentary verification, and knowledge-based authentication
Required Documentation	May be submitted after provisional enrollment; reviewed under marketplace authentication procedures	Government-issued photo ID required before account activation; sophisticated document authentication technology employed by many institutions
OFAC Screening	Not required under current marketplace regulations	Mandatory screening against SDN and sanctions lists before account opening
Credit Bureau Verification	Not required under current marketplace regulations	Standard practice; used for both identity verification and knowledge-based authentication
Real-Time Verification	Partial; provisional enrollment allowed while verification pending under current procedures	Required; account cannot be activated until identity fully verified
Fraud Detection Technology	Pattern detection capabilities; technology framework differs from banking sector	Varied deployment of advanced fraud analytics, device fingerprinting, behavioral analysis, and machine learning models depending on institution
Biometric Verification	Not used in current procedures	Increasingly adopted by larger institutions; facial recognition and liveness detection becoming more common but not yet universal
Regulatory Oversight	CMS oversight; state insurance regulators; operates under ACA statutory framework	Multiple federal banking regulators (OCC, FDIC, Federal Reserve); FinCEN; regular examinations

Dedicated Fraud Enforcement Funding	None; HCFAC funding excluded by statute	HCFAC funding available; dedicated institutional compliance budgets
Penalties for Non-Compliance	Up to $250,000 civil penalty; enforcement mechanisms structured under ACA statutory framework	Civil penalties up to $25,000+ per violation; criminal penalties up to $500,000 and 10 years imprisonment; license revocation possible
GAO Undercover Test Results	96% success rate in GAO undercover testing (23 of 24 test applications)	No comparable GAO testing; banking industry sources suggest identity fraud at account opening typically < 1% when comprehensive CIP/KYC procedures properly implemented

5.1 Key Disparities

The comparison reveals fundamental structural differences between the two regulatory frameworks:

- Verification Timing: HSA providers must verify identity before account activation under banking regulations, while ACA marketplaces operate under a framework that allows provisional enrollment with verification occurring later
- Technology Deployment: Many financial institutions employ multiple layers of fraud detection technology (though specific implementations vary), while marketplaces operate under different technological requirements
- Enforcement Structure: Banking institutions face severe penalties including potential license revocation and criminal prosecution under BSA/PATRIOT Act requirements, while ACA marketplaces operate under a different enforcement framework with no dedicated HCFAC funding
- Independent Verification: Banks typically use multiple independent data sources (credit bureaus, document authentication, knowledge-based questions), while marketplaces rely more heavily on information provided by applicants
- Compliance Culture: Financial institutions have dedicated compliance officers and fraud analysts with specialized training in BSA/AML requirements; marketplace staff operate under different training and compliance frameworks

6. Illustrative Analysis: HSA-Based Subsidy Model

6.1 Hypothetical Policy Change: ACA Subsidies Through HSAs

If federal legislation were enacted to allow or require ACA subsidies to be deposited into Health Savings Accounts rather than paid directly to insurers, applicants would encounter substantially different identity verification requirements. This section provides an illustrative modeling of how banking-sector controls might affect fraud vulnerability.

6.2 Immediate Barriers to Fraudulent Enrollment

Under an HSA-based model, someone attempting fraudulent enrollment would encounter verification barriers not present in the current marketplace system:

- Government-Issued ID Requirement: Unlike marketplace enrollment, HSA providers require submission of a valid, government-issued photo identification document. Document authentication technology employed by many institutions would likely detect altered, fabricated, or stolen identity documents
- Real-Time SSN Verification: Financial institutions verify Social Security Numbers against SSA records before account activation, with rejection of invalid numbers. The GAO testing showed fabricated SSNs were accepted by marketplace systems
- Credit Bureau Cross-Reference: HSA providers verify applicant identity against credit bureau records. Fictitious identities with no credit history—which succeeded in GAO testing—would likely fail this verification
- Knowledge-Based Authentication: Applicants must correctly answer questions based on their actual credit history. Fraudulent actors using stolen or fabricated identities would find it difficult to pass this verification
- OFAC Screening: All applicants are screened against sanctions lists, preventing accounts from being opened by sanctioned individuals
- Biometric Verification (Where Deployed): Institutions that have implemented facial recognition technology would compare live selfies to government-issued ID photos, making it more difficult to use stolen identity documents

6.3 Comparison of Fraud Scenarios

The following table illustrates how the GAO's successful test scenarios would likely fare under banking-sector HSA requirements. These are modeling projections based on typical banking procedures, not empirical test results:

GAO Test Scenario	ACA Marketplace Result	Illustrative HSA Model Projection
Fabricated SSN that failed SSA validation	Accepted in testing	Would likely be rejected - invalid SSN
Fictitious identity with no credit history	Accepted in testing	Would likely be rejected - identity not confirmed through credit bureaus or KBA

Stolen identity using real SSN	Likely accepted with limited verification	Would likely be challenged - difficulty passing KBA questions, document authentication, or biometric verification (where deployed)
Misrepresented income to qualify for subsidies	Accepted in testing - projected income used without verification	Identity verification would still be required for account opening; income misrepresentation would need to be addressed through separate eligibility controls
False citizenship documentation	Often accepted without rigorous authentication in testing	Document authentication technology employed by many institutions would likely detect altered or fabricated documents

6.4 Illustrative Fraud Reduction Modeling

Based on the comparative analysis, the following represents illustrative modeling projections rather than empirical measurements:

- GAO Undercover Testing Results: 96% of test applications succeeded (23 of 24) in the marketplace system under controlled testing conditions
- Banking Industry Estimates: Industry sources and compliance literature suggest that when comprehensive CIP/KYC procedures are properly implemented, identity fraud at account opening typically represents a small fraction of attempts—though precise industry-wide data is limited
- Illustrative Projection: Based on the structural differences in verification requirements, an HSA-based model would likely create substantially greater barriers to fraudulent enrollment than currently exist. However, the precise magnitude of improvement would depend on numerous implementation factors and cannot be empirically predicted without actual testing
- Variable Implementation: Actual results would vary significantly based on which HSA providers participate, their specific technology deployment, and the design of the policy framework

6.5 Remaining Vulnerabilities in HSA Model

While HSA account opening requirements would create additional verification layers, some vulnerabilities would remain:

- Sophisticated Identity Theft: Criminals with comprehensive stolen identity information (including ability to answer knowledge-based questions) could potentially succeed, though this represents a more challenging form of fraud

- Income Eligibility Verification: HSA identity verification does not address misrepresentation of income for subsidy eligibility determination. Separate reforms would be needed to strengthen income verification
- Insider Threats: Financial institution employees could potentially facilitate fraudulent accounts, though internal controls, auditing, and criminal penalties make this uncommon
- Variable Institutional Capabilities: Smaller financial institutions may have less sophisticated fraud detection systems than large national banks, potentially creating variability in verification effectiveness

6.6 Additional Fraud Prevention Mechanisms

Beyond initial identity verification, routing subsidies through HSAs would provide additional fraud prevention mechanisms:

- Transaction Monitoring: Financial institutions monitor account activity for suspicious patterns that could indicate fraud or money laundering
- Suspicious Activity Reporting: Banks are required to file Suspicious Activity Reports (SARs) when they detect potential fraud, creating an additional detection layer
- Ongoing Account Verification: Banks periodically re-verify customer information, particularly for higher-risk accounts or when unusual activity is detected
- Law Enforcement Coordination: Financial institutions have established relationships with law enforcement for investigating fraud, facilitating prosecution
- Account Control Mechanisms: If fraud is discovered, financial institutions have mechanisms to freeze accounts and potentially recover improper payments

7. Policy Implications and Recommendations

7.1 Revised Primary Recommendation: Integrated HSA Subsidy Framework

Congress should authorize an HSA-Based Subsidy Delivery Model that leverages existing banking infrastructure for identity verification. To ensure this does not create a barrier to entry, the following "Three-Pillar" approach is recommended:

Pillar 1: Uniform Identity Standards: Mandate that all ACA marketplace enrollments meet Customer Identification Program (CIP) standards equivalent to 31 CFR § 1020.220. This would require marketplaces to implement the same identity verification procedures that financial institutions use, including documentary verification, non-documentary verification, and risk-based procedures.

Pillar 2: Automated Eligibility Bridging: Develop a real-time API between marketplaces and financial institutions to confirm identity verification results instantly, preventing "provisional enrollment" windows that GAO testing showed were exploitable. This would ensure that subsidies are not committed until identity has been fully verified through banking-level procedures.

Pillar 3: Public-Private Safety Net Accounts: For "unbanked" or "high-risk" individuals (e.g., those in ChexSystems), establish a government-backed "Standard HSA" with restricted features but full KYC compliance to ensure healthcare access is not denied based on banking history. This pillar is essential to prevent the HSA-based model from creating barriers to coverage for vulnerable populations while still maintaining identity verification integrity.

Pillar	Objective	Mechanism	Key Benefit
1. Uniform Identity Standards	Eliminate verification gaps	CIP requirements per 31 CFR § 1020.220	Closes loopholes exploited in GAO testing
2. Automated Eligibility Bridging	Eliminate provisional enrollment exploitation	Real-time API between marketplaces and financial institutions	Prevents subsidy commitment before verification
3. Public-Private Safety Net	Ensure universal access	Government-backed Standard HSA for unbanked individuals	Maintains healthcare access while preserving integrity

7.2 Strengthening Income Verification Mechanisms

While the HSA model excels at identity verification, it does not inherently solve income misrepresentation. The GAO testing and subsequent analyses have shown that income verification remains a critical vulnerability. To address this:

Real-Time Data Access: Legislation should grant marketplaces broader access to current-year payroll data (e.g., via The Work Number or similar services) to move away from the "projected income" attestation model. This would allow verification of actual current income rather than relying on applicant projections that cannot be verified until tax reconciliation occurs the following year.

Tiered Verification: If an applicant's self-reported income deviates by more than 10% from the most recent IRS data, "hard-stop" documentation (such as recent pay stubs) must be verified through sophisticated document authentication before subsidies are committed. This tiered approach balances administrative efficiency for straightforward cases with enhanced scrutiny for higher-risk applications.

Verification Element	Current ACA Process	Recommended Process
Income Data Source	IRS data (1-2 years old); self-attestation for current year	Real-time payroll data via Work Number or similar; IRS data as backup
Verification Trigger	Large discrepancies may trigger documentation request (inconsistently applied)	Automatic hard-stop for >10% deviation from IRS data
Document Authentication	Manual review with limited authentication technology	Sophisticated document authentication (OCR, security features, fraud detection)

7.3 Enforcement and Transparency Reforms

To fix the "Enforcement Gap" between the banking sector and the ACA marketplace, the following legislative and regulatory reforms are recommended:

Expand HCFAC Jurisdiction: Amend 42 U.S.C. § 1320a-7c to allow Health Care Fraud and Abuse Control (HCFAC) funds to be used specifically for ACA marketplace and APTC investigations. This would bring the proven fraud prevention infrastructure—which delivers $4-8 return on investment for Medicare and Medicaid—to the ACA marketplace. Currently, OIG cannot use HCFAC funding for marketplace fraud, creating a critical enforcement gap.

Mandatory Investigative Disclosure: Require CMS to publish summarized findings for any agent/broker suspension lasting more than 30 days. This would prevent the "reinstatement without disclosure" pattern observed where 850 brokers were reinstated despite 160,000 likely unauthorized changes identified by GAO. Transparency in enforcement actions would deter future misconduct and allow state regulators to take appropriate parallel actions.

Establish a Marketplace Strike Force: Model a dedicated investigative team after the HEAT Strike Force, which has charged over 5,800 defendants in Medicare/Medicaid

contexts, to focus exclusively on systemic enrollment fraud schemes. The Strike Force should include dedicated prosecutors, investigators from HHS-OIG and DOJ, and data analysts with authority to pursue multi-state fraud rings targeting the ACA marketplace.

Reform	Current Gap	Expected Impact
Expand HCFAC Jurisdiction	HCFAC funding cannot be used for ACA marketplace fraud	Access to proven fraud prevention infrastructure with $4-8 ROI
Mandatory Investigative Disclosure	850 brokers reinstated without public disclosure of findings	Deterrence through transparency; coordination with state regulators
Marketplace Strike Force	Fewer than 10 federal prosecutions despite 275,000+ complaints	Dedicated resources modeled on HEAT Strike Force (5,800+ defendants charged)

7.4 Implementation Considerations

Successful implementation of these recommendations would require addressing several operational challenges:

- HSA Eligibility Requirements: Current law requires HSA holders to have high-deductible health plans. Legislation would need to modify HSA eligibility rules to accommodate ACA marketplace plans or create a similar account type with banking-level verification requirements
- Unbanked Populations: The Public-Private Safety Net (Pillar 3) must be designed to provide equivalent access for individuals without traditional banking relationships, including those flagged in ChexSystems
- Administrative Coordination: Systems would need to be developed for marketplaces to communicate with financial institutions regarding subsidy amounts and eligibility changes via the real-time API (Pillar 2)
- Consumer Education: Beneficiaries would need education about managing HSA accounts and using subsidy funds for premium payments
- Phase-In Period: A gradual implementation would allow systems and procedures to be tested and refined before full-scale deployment
- State Coordination: The 20 states operating their own marketplaces would need to implement compatible systems, though many already have stronger verification than the federal marketplace

7.5 Cost-Benefit Considerations

While enhanced verification procedures would increase administrative costs, the benefits would likely substantially exceed expenses:

- Fraud Reduction Savings: Reducing fraudulent enrollment would save improperly paid subsidies. With $124 billion in subsidies paid in 2024 and estimates of improper enrollment ranging from 1.5% (GAO-identified unauthorized changes) to potentially much higher, even modest fraud reduction would generate substantial savings
- Economies of Scale: Banking institutions have already made capital investments in fraud prevention technology; leveraging these systems through Pillar 2 would be more cost-effective than building equivalent systems from scratch
- Program Integrity Benefits: Stronger fraud prevention would improve public confidence in the ACA marketplace system and reduce political pressure to eliminate subsidies entirely
- HCFAC Return on Investment: Medicare fraud prevention activities consistently return $4-8 for every $1 spent. Extending this infrastructure to the marketplace could generate comparable returns
- Competition Effects: Financial institutions would compete to attract HSA account holders, potentially driving innovation in services and reducing account fees

8. Summary of Findings

This analysis has demonstrated that:

- The ACA marketplace enrollment system, while complying with its current statutory and regulatory framework, demonstrated vulnerabilities in GAO undercover testing (96% test success rate in 2023; 90% of fictitious applicants still receiving coverage in 2025)
- These vulnerabilities stem from reliance on attestation-based verification, limited real-time cross-checking, and different technological requirements than banking-sector systems
- A critical structural limitation is the exclusion of ACA marketplace fraud from HCFAC funding, leaving no dedicated federal enforcement funding stream comparable to Medicare/Medicaid fraud prevention
- Criminal prosecution of ACA enrollment fraud has been minimal—fewer than 10 federal cases through 2025 despite 275,000+ consumer complaints in 2024 alone and GAO identification of 160,000 likely unauthorized broker changes
- Financial institutions opening HSAs employ comprehensive identity verification procedures mandated by BSA/PATRIOT Act requirements and backed by severe penalties for non-compliance
- The banking sector's regulatory framework, including KYC, OFAC screening, and mandatory CIP procedures, creates multiple verification layers not currently required in marketplace enrollment
- The Three-Pillar HSA framework, combined with income verification reforms and expanded HCFAC jurisdiction, would address the identified vulnerabilities while maintaining healthcare access for all eligible Americans

9. Conclusion

The GAO undercover investigation revealed that 96% of test applications succeeded in the ACA marketplace, highlighting vulnerabilities in current enrollment procedures. This report's comparative analysis demonstrates that the disparity between ACA marketplace verification procedures and financial institution account-opening requirements reflects a fundamental difference in regulatory frameworks and technological capabilities.

Financial institutions operate under a comprehensive regulatory framework that mandates robust identity verification, creates multiple layers of fraud detection, and enforces compliance through severe penalties, including criminal prosecution and license revocation. The HEAT Strike Force has charged over 5,800 defendants in Medicare/Medicaid fraud cases since 2007. In stark contrast, ACA marketplace fraud enforcement has resulted in fewer than 10 federal prosecutions despite 275,000+ consumer complaints in 2024 alone.

The exclusion of ACA marketplace fraud from HCFAC funding creates a critical enforcement gap. The proven fraud prevention infrastructure that delivers $4-8 return on investment for Medicare and Medicaid is unavailable for the marketplace. Meanwhile, 850 brokers suspended for suspected fraud were reinstated without public disclosure of investigative findings, and GAO identified 160,000 likely unauthorized broker changes in 2024.

This analysis recommends a comprehensive Three-Pillar approach: (1) Uniform Identity Standards requiring CIP compliance equivalent to 31 CFR § 1020.220; (2) Automated Eligibility Bridging through real-time API verification to eliminate provisional enrollment exploitation; and (3) Public-Private Safety Net Accounts to ensure healthcare access for unbanked populations while maintaining verification integrity.

Additionally, income verification must be strengthened through real-time payroll data access and tiered verification with hard-stop documentation requirements. The enforcement gap must be closed by expanding HCFAC jurisdiction to include ACA marketplace fraud, mandating disclosure of suspension findings, and establishing a dedicated Marketplace Strike Force modeled after the successful HEAT program.

Implementation challenges exist, particularly regarding HSA eligibility requirements and serving populations without traditional banking relationships. However, the Three-Pillar framework specifically addresses these concerns through the Public-Private Safety Net. The alternative—maintaining current marketplace procedures—leaves vulnerabilities that GAO testing has repeatedly demonstrated can be exploited, with 90% of fictitious applicants still receiving subsidized coverage as of late 2025.

This analysis supports comprehensive policy reforms that adopt banking-level verification standards, strengthen income verification, and close the enforcement gap through expanded HCFAC jurisdiction and a dedicated Marketplace Strike Force. These reforms would substantially reduce vulnerability to fraudulent enrollment while preserving access to healthcare subsidies for legitimately eligible Americans.

Appendix: Regulatory Citations

Key Federal Statutes and Regulations

Government Accountability Office Report:

- U.S. Government Accountability Office. Patient Protection and Affordable Care Act: Preliminary Results from Ongoing Review Suggest Fraud Risks in the Advance Premium Tax Credit Persist. GAO-26-108742. Washington, D.C.: December 3, 2025.

ACA Fraud Enforcement Authority:

- 42 U.S.C. § 18081 (Section 1411 - Procedures for determining eligibility)
- 45 CFR § 155.285 (Civil penalties for false or fraudulent information)
- 31 U.S.C. § 3729 et seq. (False Claims Act)
- 42 U.S.C. § 1320a-7 (Exclusion of certain individuals and entities from participation)

Health Care Fraud and Abuse Control (HCFAC):

- 42 U.S.C. § 1395i (Medicare Trust Fund)
- 42 U.S.C. § 1320a-7c (HCFAC Program)
- Note: HCFAC funding is currently limited to Medicare and Medicaid program integrity activities

Bank Secrecy Act:

- 31 U.S.C. §§ 5311-5332
- 31 CFR Chapter X (FinCEN regulations)

USA PATRIOT Act:

- Section 326: Customer Identification Programs (codified at 31 U.S.C. § 5318(l))
- 31 CFR § 1020.220 (Customer Identification Program requirements for banks)

OFAC Regulations:

- 31 CFR Chapter V (Office of Foreign Assets Control)
- 50 U.S.C. § 1701 et seq. (International Emergency Economic Powers Act)

Affordable Care Act:

- 42 U.S.C. § 18001 et seq.
- 45 CFR Part 155 (Marketplace regulations)

Health Savings Accounts:

- 26 U.S.C. § 223
- IRS Publication 969