Before the Mandates Land

PREPARING SOS OFFICES FOR BUSINESS IDENTITY THEFT REFORM

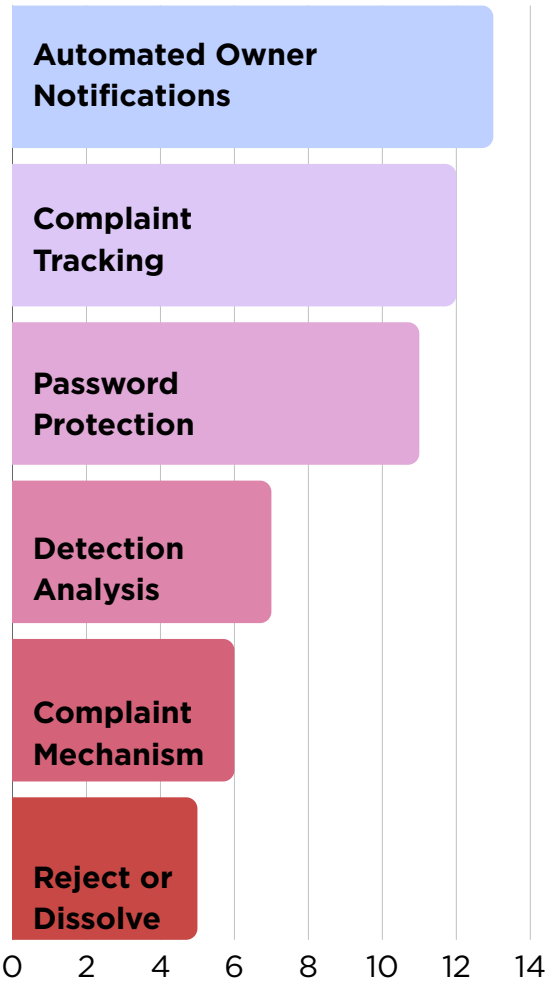
Since 2022, states are passing more laws creating complaint mechanisms, expanding Secretaries of State (SOS) authority to investigate and fix fraud, and requiring coordination with attorneys general.

Yet these reforms only formalize the work many offices already absorb in response to business identity theft (BIT), and they land hardest on offices whose filing systems weren't built for adversarial conditions.

Now is the time to understand the current BIT threat landscape, and adopt a framework to assess and strengthen your office's ability to respond.

Why Legacy Systems Risk Exposure

Most filing systems were built for efficiency and accessibility, not high-speed fraud. A National Association of Secretaries of State (NASS) survey found 83% of offices don't track BIT complaints, so the scale of the problem is largely invisible inside the very offices required to address it. New statutory duties will redirect rather than remove this workload, straining systems already operating without the tools to detect or reverse fraud.



Modern SOS responses to business filing fraud (2025 NASS survey)

Where Threats Meet Vulnerabilities

Each attack vector exploits a specific gap in how filing systems were designed:

- **Entity hijacking succeeds** because systems lack real-time identity verification and automated owner notification. Filers are accepted at face value, and legitimate owners learn of unauthorized amendments only after the damage is done.

- **Synthetic identities exploit** weak authentication and limited pattern detection. Knowledge-based verification is easily defeated, and batch processing can't flag the rapid, coordinated filings that build and dissolve shell entities.

- **AI forgeries overwhelm systems** that depend on manual review. Without strong upfront verification, convincing documents and IDs pass through, and inadequate audit trails make the fraud hard to trace and reverse.

- **Record exploitation is fueled by personally identifiable information (PII)** exposed in public filings. Sensitive identifiers harvested from the record itself become the raw material for future attacks.

How SOS Offices Strike Back

The NASS survey found at least **20 states pursuing technology to combat business filing fraud.** Modern systems give SOS offices capabilities that established architectures can't support:

API-based identity verification
connects to third-party proofing services

Real-time fraud analytics
scores filing velocity, IP reputation, and change clustering

Automated owner notifications
alerts sent immediately when changes are filed

Immutable audit trails
support investigation and rollback

PII minimization
auto-redaction and document watermarking

Complaint tracking
puts an SOS office ahead of 83% of their peers

Assessment & Action Framework

Knowing where your office stands, both technically and organizationally, is the first step toward preparedness for business identity theft legislation.

Detection	Notification	Reversal	Documentation	Readiness
Can your system verify filer identity or flag suspicious patterns?	How quickly can business owners be notified of changes? Is it automatic?	Can you cancel, redact, or flag records without manual editing across systems?	Can you pull and match filings fast enough for investigations?	What sensitive identifiers are visible in public records?

How many hours do staff spend on workarounds?	How well are BIT complaints currently tracked, if at all?	How much time goes to chargeback or ACH-related issues?	Who has critical institutional knowledge? How will they shape implementation?	What training will staff need to adopt new tools confidently?

About Reframe Solutions

ReFrame Solutions equips government and education partners with purpose-built software and reliable teams they can count on, giving them the confidence to deliver outcomes the public can trust.

ReFrame SOLUTIONS

reframesolutions.com
844-4-REFRAME
844-473-3726