NASS Business Identity Theft Task Force: Findings & Suggestions for States

In collaboration with IACA, NASS surveyed Secretary of State offices on state practices in tracking, reporting and addressing issues related to business identity theft. Based on the responses provided, a majority of Secretary of State offices (83% of respondents) are NOT tracking business identity theft complaints, instead relying upon externally-generated law enforcement reports and other forms of information-sharing. More than half of all SOS offices that took part in the survey (61%) said they could not provide data on the number of business identity theft complaints that were received in the past year.

As a result of the survey findings and state discussions with public and private-sector experts, Secretary of State offices may want to consider one or more of the following practices:

#1: Internally track data that is critical to addressing business identity theft issues.

Examples of data that states are currently tracking:

- Complainant Name / Complaintee Name (who is being complained about)
- SOSID Number (identification number for the entity that is the focus of the complaint)
- Received Date
- Staff Assigned (for internal accountability) with Date of Assignment
- Status of Complaint (to track level of completion)
- Description of Complaint
- Action Summary (agency action, including forward to law enforcement, Attorney General, etc.)
- Submission of Affidavit (to affirm the person claiming legitimate control of the entity in order to cancel a false filing, etcetera)
- Interrogatories and Due Date (if unanswered, can result in the administrative dissolution of the suspicious entity)
- Payment Type (fraud often discovered through bad payment method)
- Account Holder Name
- Name of Individual Signing Payment Method
- Source of Complaint (internal discovery vs. external complaint)

#2: Implement tools or identifiers that help to determine problem entities across the agency, or as is the case with states like Colorado, assign identifiers for use across all state agencies.

- Database management tools, such as a color-coded system that visually flags an entity as a problem (North Carolina), can help to identify problem entities across the state agency.
    - Red flag = Stop and do not allow any additional filings (nonpayment issues)
    - Blue flag = Check with supervisor before proceeding with filing

- Software can identify when an address is not a valid address according the U.S. Postal Service (USPS), preventing bad addresses from entering the system.

#3: Track "benchmark" data points associated with fraud activity to be centrally kept and reported.

This information, which can highlight increasing rates of state/regional problems, should include:

- Rate of bad payments
- Rate of expedited reinstatements

#4: Provide clear remedies for remediation of fraudulent filings.

The most prominent options that states currently have in place to address fraudulent filings and/or business identity theft include:

- Referral to the Office of the State Attorney General (39% of IACA survey respondents)
- Email alerts/text alerts or a monitoring service for electronic filings (28% of survey respondents)
- Administrative/affidavit process for victims of business identity fraud/theft to cancel fraudulent filings (22% of survey respondents)

#5: Take the lead on state discussions about current laws and legal penalties for addressing business identity theft.

In general, most cases of business identity theft are prosecuted under fraud and theft statutes. About a third of all state survey respondents (29%) noted that they have no specific laws to address business ID theft, while several respondents pointed to state code prohibiting the signing of false documents. Additionally, no state currently has a law preventing someone previously charged with criminal misuse of corporate entities from serving as a manager or a director for another state entity, although states such as Oregon reported that state courts and the Attorney General have, on rare occasion, ordered a person to refrain from doing business in their state. Of course, simply being able to query the state database for such information may be a major solution to preventing business fraud issues by repeat bad actors.