northwest
REGISTERED AGENT

Playing the Long Game:

Fighting Fraudulent Business Filings through Modernization

When fruit sits out for too long, it quickly turns from fresh to rotten. If left to sit in this state, it will eventually attract a swarm of fruit flies. Technological security is quite similar. A platform that was secure when first developed goes from new to outdated to obsolete almost as quickly as fruit goes bad. However, instead of just dealing with annoying fruit flies, outdated tech attracts bad actors and fraudsters that can easily circumvent security and manipulate systems to their owns ends. This is exceptionally true in the world of state business filings. Many states are using outdated filing platforms, and, unsurprisingly, many states are also combating an influx in fraudulent filings. Once a state becomes the target of fraudsters, the initial reaction is usually to investigate and stop the bad actors then form working groups to discuss future legislative solutions. While these steps are important, they divert finite state resources away from the technological modernization that is required to prevent future instances. Without modernizing their filing platforms, states will always remain several steps behind fraudsters. Thus, states should focus on this much needed technical modernization and partner with the registered agent ("RA") community to help stymie the issue rather than attempting to fight fraud alone.

API: Application Programming Interface Authentication Prevents Incursion

For years, API (or Application Programming Interface) has been little more than a buzzword surrounding state filings systems with few states actually achieving some level of API integration. While most know that API is a feature that can be used to streamline filings via system to system communications, the ability of API to reduce fraud via enhanced authentication measures must be highlighted. The ability of API systems to include and streamline authentication make it an instrumental weapon in the battle against fraudulent filings.

Essentially, API authentication is "the process of verifying the identity of a user or system making a request" to another API user or system.[1] Rather than a simple login and password, API authentication helps maintain "the security and integrity of the API, ensuring that only authorized entities can access its features and interact with the underlying data or services it provides."[2]

Authentication occurs in multiple ways, with identity verification usually being the first step. This is typically achieved through various methods, such as API keys, various types of tokens, or other credentials.[3] Identification not only allows API platforms to better control who has access, but also what systems within the platform they have access to. Thus, a multitude of information can be housed within the same platform without the need to worry about who can access what.[4] Access controls can include safeguards like limit requests/throttling, which can reduce the scraping of data or DDoS attacks[5], and session management, which sets parameters around repeat access before re-identification is needed.[6]

Perhaps the most important feature of API authentication is the ability to see who is accessing the platform, what are they doing, and when are they doing it. By providing a more robust set of analytics, those maintaining an API platform can easily observe interactions, view trends, and test and prepare for potential security risks in ways that outdated platforms simply cannot hope to match.[7] This type of monitoring is instrumental in reducing and preventing fraud. Teams can identify suspicious behavior in real time and cutoff access as problems develop.

A perceived drawback of implementing any new security measure is how it will impact the user experience. Filing delays are a major driver of communications to any state's business division. Couple delays with more intricate technological steps in order to submit a filing and one could assume that communications, especially aggravated communications, would drastically increase. While an increase in communications is expected with any platform change, growing public awareness of fraud and identity theft have created a significant level of acceptance and understanding when it comes to the need to protect transmitted information. For most, a short delay or added processes are a small price to pay for security, a sentiment reinforced by a recent study suggesting that "91 per cent willing to take extra

1 *API authentication - A key to combating fraud risks,* FRAUD.COM (2024), https://www.fraud.com/post/api-authentication.
2 *Id*.
3 *Id*.; *see also* Daniel Strebel & Varun Krovvidi, *Unpacking API Management policies [Part 2]: 5 ways to handle REST API authentication*, GOOGLE CLOUD BLOG (Feb. 8, 2023), https://cloud.google.com/blog/products/api-management/5-ways-to-implement-rest-api-authentication.
4 *Supra*, note 1.
5 Hassene Belgacem, *API Security Best Practices? Part 1/6-Access control*, MEDIUM (Dec. 4, 2022), https://medium.com/@hassene/how-to-secure-your-api-part-1-6-access-control-best-practices-311ac29d7f6c.
6 *Supra*, note 1.
7 Caitlin Halla, *API Monitoring Explained: How To Monitor APIs Today*, SPLUNK BLOGS (Mar. 26, 2025), https://www.splunk.com/en_us/blog/learn/api-monitoring.html; *see also What Is an API Security Audit?*, AKAMAI, https://www.akamai.com/glossary/what-is-an-api-security-audit.

security measures to prove their identity on an ongoing basis to protect their information and accounts."[8]

BAD ACTORS TARGET OUTDATED SOFTWARE

In 2019, the cities of Baltimore, Maryland, and Greenville, North Carolina, were both the victims of "ransomware" attacks by malware named "RobbinHood."[9] According to Lawrence Abrams, founder of technology news site Bleeping Computer, "[t]he creator or creators of RobbinHood most likely scanned a large number of online systems for vulnerabilities to exploit, such as gaps in protocols used to grant remote access to computers."[10] This reasoning is crucial in understanding fraud: if Baltimore and Greenville were simply targeted because they were vulnerable, any state, locality or agency could be a target if not properly maintaining their software and systems.

The cost of software upgrades coupled with the general public's lack of high-level technological understanding make postponing upgrades easy, especially when state and local governments have so many other issues to address. However, postponement is too often an endless cycle, and, rather than breaking that cycle, states often focus on their fraudulent filing issues by enacting legislation or forming working groups to evaluate various causes contributing to the problem. While these steps may help in the short term, failure to modernize their filing systems is akin to leaving a piece of fruit on the counter while you attempt to swat each buzzing fly.

REGISTERED AGENTS CAN HELP SHOULDER THE BURDEN

The client/RA relationship is one built upon trust and security. However, because RA (specifically commercial RA) information can be easily located online, they are often victims of fraudulent filings and appointed without their consent. Therefore, RAs have their own vested interest in preventing fraudulent filings, as it protects their brand, saves money, and reduces potential liability.

While focusing on modernization, states can take immediate action in the fight against fraud by leveraging the RA community. For starters, states can periodically send RAs a list of all the business entities that have appointed them and allow agents to deny consent on fraudulent appointments. This level of communication and cooperation is essential to effectively fight fraud. RAs could opt into receipt of these lists and states could provide them under the "prescribe procedures that are reasonably necessary to perform the duties required of the secretary of state" language found in business divisions' enabling statutes.

---

8 George Hopkin, *Outdated cybersecurity tech "betrays the trust of consumers"*, TECH. MAG. (Nov. 23, 2022), https://technologymagazine.com/articles/outdated-cybersecurity-tech-betrays-the-trust-of-consumers.

9 Niraj Chokshi, *Hackers Are Holding Baltimore Hostage: How They Struck and What's Next,* N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

10 *Id*.

The ability for RAs to deny their appointment if made without their consent is also crucial to fighting fraud. Several states have implemented procedures for such denial, but they need to be adopted on a much larger scale. RA Resignation is simply an inefficient vehicle to address the situation due to the often more than 30 day timing elements in most resignation statutes. In some states, the creation of a denial of RA consent filing would be permissible under the same type of enabling statute referenced above. In others, such a filing may need to go through the appropriate administrative procedures.

Another potential solution is for all states to adopt a uniform mechanism that allows or requires a RA to accept their appointment by an entity. States could send an email to the newly appointed RA requiring the RA to affirmatively accept the appointment. The process could be inverted as well to reduce filing rejection and re-submission rates. RAs could be informed of their appointment and have a short window to reject the appointment and nullify the filed document. Unfortunately, though this is the most secure option, it more than likely would require legislative changes.

CONCLUSION:

Fraudulent filings are increasing across the country, and, due to outdated state filing platforms, the problem is almost impossible to contain. States should devote resources toward modernizing filing platforms, while working with RAs to help in the collective fight against fraud. By working together on the issue, state business services divisions and RAs can finally keep the flies at bay.