Empowering people who serve the public®

tyler technologies

ISSUE PAPER

Securing the Future: Strategies for Fraud Monitoring and Prevention

Ron Thornburgh, Vice President of Digital Government Policy & Advocacy, Tyler Technologies

ISSUE PAPER

Securing the Future: Strategies for Fraud Monitoring and Prevention

INTRODUCTION:

Since the earliest days of government, the fundamentals of public records and the need for their security have remained constant.

Yet the methods and strategies to achieve this security have evolved with the changing threats governments face, which are now greater than ever.

Reflecting on this evolution, two fundamental questions arise. First, are state systems capturing and managing the right digital information? This is a vital question since extraneous data can present unnecessary risks. Second, how do state systems balance the need for public access to records with the imperative to maintain the security and privacy of those records and their filers? This delicate balance is a daily challenge that impacts every filing by the public.

This issue paper focuses on a crucial aspect of ensuring this security: fraud monitoring and prevention.

IMPORTANCE AND FEASIBILITY OF FRAUD MONITORING AND PREVENTION

During the dawn of the digital government age, the primary security concern was protecting individual documents and pieces of information. Today, the scope of threats has multiplied exponentially. State systems must now defend against relentless distributed denial-of-service (DDoS) attacks, sophisticated phishing schemes, and dangers posed by both external and internal bad actors. These threats are not only more frequent but also more varied, with vast amounts of data targeted and entire systems held hostage.

The most prevalent forms of fraud we are witnessing today — especially regarding business licenses — revolve around identity theft. The motive often involves hijacking corporate identities to conduct financial crimes like money laundering or credit fraud. The threat has become more viable for bad actors and has made fraud monitoring not just necessary but imperative.

One fundamental security measure is the tracking of corporate ownership and changes. In Arkansas, for example, business owners can subscribe to a change monitoring feature for a nominal annual fee of $5. The feature performs a daily check for any modifications to their corporate online filing. Any changes trigger immediate notifications, allowing for swift action against unauthorized changes. To date, 15,000 users in Arkansas have signed up for the service.

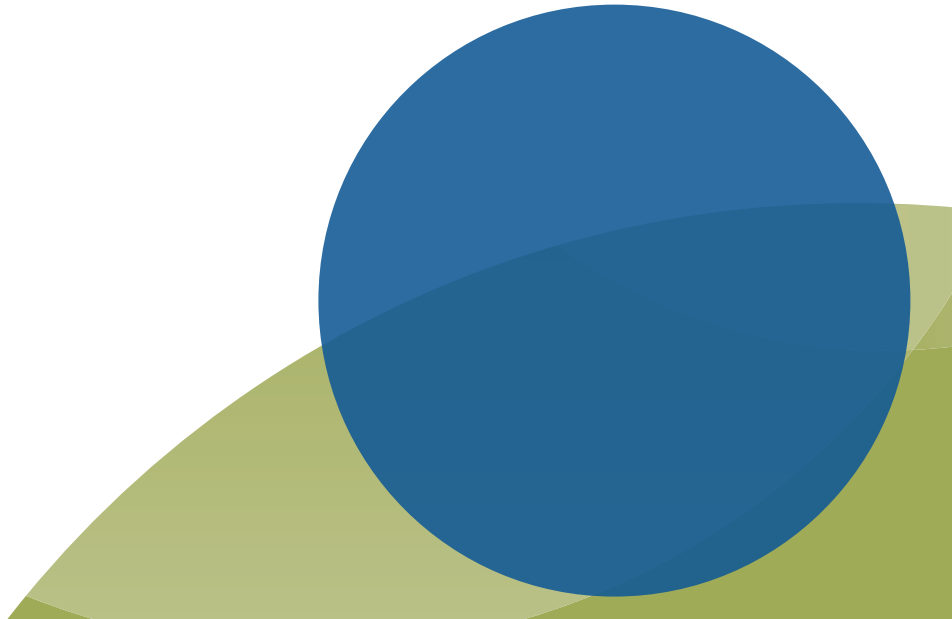
This kind of fraud monitoring system is a layer of protection that guards against not only the theft of a company's identity, but also the potential financial crimes that could follow. It's an approach akin to personal credit or identity theft protection services, but tailored for business entities.

The U.S. Department of Treasury now requires beneficial ownership information to be filed with the Financial Crimes Enforcement Network (FinCEN). This is a significant move toward national consistency in combatting fraud. Although this new requirement has introduced some complexity at the state level, it is a clear indication that the federal government recognizes the seriousness of the issue.

Looking ahead, one policy shift to advocate for is the integration of uniform commercial code (UCC) records with corporate filings to enhance fraud monitoring. If any alterations occur to a UCC filing, which indicates a lien against a corporate entity's property, both the entity and the bank should be notified.

In essence, the role of state systems has evolved from being mere repositories of public records to being active custodians of data integrity. The notion that once a document was filed it would be untouched in a filing cabinet is antiquated. With the modern threats we face, states have an opportunity to alert the owners of records to any and all changes, thereby preventing fraudulent activities before they can cause harm.

This proactive stance on fraud monitoring and prevention is not only about keeping pace with fraudsters but also about outsmarting them. The monitoring technology is there — it's accessible, it's doable, and in the context of the risks we face, it's indispensable. The future security of state systems depends on the implementation of real-time monitoring systems that can adapt as quickly as the threats they're designed to thwart.



SEVEN RECOMMENDATIONS FOR IMPROVING FRAUD MONITORING

Recommendations for enhancing fraud monitoring must address security threats head-on. In recognition of the importance of this endeavor, the recommendations below are made with the following acknowledgment: While bad actors need only a single lucky break, our systems must strive for perfection in protection.

1. Advanced Real-Time Monitoring Systems

Putting in place advanced real-time monitoring systems, like those used in Arkansas, can serve as a model for all states. For a nominal fee, businesses can have the security of knowing that any change to their corporate filings will trigger an immediate notification, allowing them to take swift action against fraudulent changes.

2. Uniform Commercial Code Monitoring

Expand monitoring efforts to include UCC filings tied to corporate entities. Any changes to these filings — such as a lien against corporate property — should automatically notify the business owner, allowing the owner to quickly identify fraud.

3. Comprehensive Data Strategy

Develop a comprehensive data strategy that goes beyond mere collection. It should focus on the relevance, protection, and appropriate use of data. The strategy should prioritize securing the data that is most valuable and at the highest risk. It should also ensure that state systems are not holding unnecessary information.

4. Cross-Agency Cooperation

Encourage a cooperative environment across state agencies, local governments, and private-sector partners. By tapping into resources that already exist, states can enhance their fraud monitoring capabilities without reinventing the wheel.

5. Cost-Effective and Secure Solutions

Pursue solutions that are not only faster, better, and cheaper but also more secure. Investments in technology should be made with a clear understanding of their impact on public policy and service delivery, ensuring that they serve residents and businesses effectively.

6. Public-Private Technology Partnerships

Leverage public-private technology partnerships to access innovation and expertise available in the private sector. This includes working with companies that can provide the best technology solutions and share their insights to enhance state systems' security.

7. Public-Centric Experience

Adopt a public-centric experience that eliminates the need for users to navigate through a maze of government agencies. Centralizing services through a secure online portal creates a more streamlined experience for individuals and businesses alike.

CONCLUSION

As we look to the future, policies and practices must evolve to address not only the current landscape of security threats but also anticipate new ones. By adopting these recommendations, state systems can protect themselves against fraud more effectively, offering peace of mind to both the government and the public it serves. States should know they are not alone in the fight against fraud and that there are numerous resources available, from state CIOs to private-sector partners like Tyler Technologies.

For additional insights, visit Tyler's Resource Center at tylertech.com.

ABOUT TYLER TECHNOLOGIES, INC.

Tyler Technologies (NYSE: TYL) provides integrated software and technology services to the public sector. Tyler's end-to-end solutions empower local, state, and federal government entities to operate efficiently and transparently with residents and each other. By connecting data and processes across disparate systems, Tyler's solutions transform how clients turn actionable insights into opportunities and solutions for their communities. Tyler has more than 40,000 successful installations across nearly 13,000 locations, with clients in all 50 states, Canada, the Caribbean, Australia, and other international locations. Tyler has been recognized numerous times for growth and innovation, including Government Technology's GovTech 100 list. More information about Tyler Technologies, an S&P 500 company headquartered in Plano, Texas, can be found at tylertech.com.

NASS-WP-33192-0124