From: Pappalardo, Janine
To: Public Comment SB22034
Subject: [EXTERNAL] Public Comment for Fraudulent Filing Working Group Meeting
Date: Wednesday, September 14, 2022 3:03:43 PM
Attachments: image001.png

Hello,

On behalf of Experian, I would be delighted to offer our credentials and bona fides in the domain of fraud prevention and detection. In deference to the working group's time and sensibilities, I will simply state that we have established a reputation as a leader in the world of fraud prevention and detection.

Based on our experience in combatting identity and commercial fraud, Experian offers the following input which bolsters some points made in the very first Fraudulent Business Filings Working Group session made by Greg Wertsch, House Speaker Appointee, Special Agent, U.S. Department of Homeland Security. The points made were aimed at addressing fraud attempts up front at the outset of online, digital interactions and included:

- Making it more difficult for a fraudster to open the business by authenticating the filer online and at the onset of the process
- Using an algorithm to flag fraud
- Improve the data marketplace to look for red flags, improve data resolution and linkage across databases for quicker access to more accurate information

These are all areas where Experian has significant expertise and experience and can attest that an emphasis and focus in these areas will provide the State of Colorado with the most significant return on investment, and protect the State, its business owners and registrants and reduce the strains and expenses of current workflow processes.

It is our experience that the efforts to verify a filer's identity when they are attempting to gain access to the system of record are critical when at the frontend. This helps in two ways. First, this can quickly identify and stop potential bad actors at the point of entry. Secondly, for those actors that are part of an organized effort, they will recognize the new scrutiny and rigorous methodology of identity authentication. This often motivates the actor(s) to move on from the State's site to other, less secure sites.

Online identity verification services are fairly commonplace with online transactional sites for entities including financial services, banks, online retailers and even many government operations. Costs for such services vary on the level of capability required but are generally between $0.35 - $1.30 per transaction. Our advice is that any such service is optimally viewing the identity as both the individual (as determined by unique attributes or combination of attributes) and the device (as determined by unique attributes or combination of attributes). In this way, the State can assess the individual and device as well as the combination of devices. There are well established and proven online identity verification services that can provide a risk assessment of the individual by virtue of attributes such as PII, email address, mobile phone and/or step-up authentication methods such as multi-factor-authentication/one-time-passcodes. Likewise, equally well-established services exist that discretely interrogate the devise for attributes to create a 'device print' which acts like a unique fingerprint for the device. These device attributes can then be assessed to produce an overall device

risk score by considering things like geo-location, IP address, device masking and other anomalies. All of the verification mentioned above for both the individual and device is conducted online during the interaction with the filer in real or near-real-time. Typically, clients have a business process to handle those individuals who fall out of the process and still pursue completing the transaction as they are legitimate filers. It is our experience that fraudsters do not continue to pursue the transaction in an out-of-band situation. It is also worth noting that these services are generally tailorable to adjust the stringency of the risk assessment to meet the clients balance of friction with risk. We regularly work with clients to tune these services based on an analytical feedback loop to eliminate, to the extent feasible within the client's risk tolerance, the occurrence of false positives. It is our view these services should be optimized to allow you legitimate and good customers to get through the verification but stop the bad actors. This is a balancing act we help our clients manage every day.

We also urge our clients when evaluating the digital identity of a commercial entity to assess that identity with information from across a wide range of channels. There is technology available today which can perform risk assessments on the entity by looking at firmographic data, credit data as well as signals in a variety of ways including things like website traffic trends, advertising activity and SEO activity all of which would indicate a healthy and legitimate business. Some services include weighted risk scores which can provide an indication of risk across a spectrum. We recommend assessing ownership where available and the linkage of ownership across multiple entities. Simply verifying a business name or address is a foundational step but hardly adequate by itself given the fraud strategies that continue to exist and more importantly, evolve over time. Multiple data sources, multiple signals and real-time assessment are critical factors in combatting commercial fraud.

Because of the evolving nature of the risk, static risk scores are limited in effective over time. It is important to ensure that the services employed that use a modeled risk score have the ability to be validated and updated over time. As important is the ability for the model or model provider to incorporate new or additional data in the model. Our direct experience has been that our own models can be tailored with non-Experian data to improve performance in risk determination and increase our client's confidence in the model's performance. While the State can commission custom built models and algorithms, the cost savings to modifying and leveraging existing already tailored and pre-built solutions offer significant savings. In our experience this approach also leverages the experience of our exiting clientele.

We encourage our clients to also ensure their approach is not static over time and that performance of strategies and methods are evaluated in a data driven analytical approach. We work with our client's to develop a closed loop analytical process where results are provided in terms of false positive and negative performance. This feedback loop helps inform the next generation of model tailoring or strategy development.

We again commend the State of Colorado's advancement on this issue and the commitment to address fraudulent filings. Fraud in this area can be detrimental to so many citizens. Once a fraudster harms an existing, valid business, or even worse, is somehow able to obtain a fraudulent registration from the state to commit wrongdoings under the fraudulent business name the damage is already done and, in the case of the latter, the limit to that damage is limitless until stopped.

The easiest and most secure way to address fraud is to stop it before it happens.

Thank you for your continuing efforts on behalf of the State of Colorado citizens, businesses and for all citizens and businesses out of state as well that could also be impacted.

Best Regards,

Janine Pappalardo
Account Executive – Public Sector, State and Local
555 12th St. NW, [redacted] Washington, D.C., 20006
[redacted]

Learn about Experian Public Sector solutions