From: Roger Loeb
To: Public Comment SB22034
Subject: [EXTERNAL] Excellent first meeting...
Date: Wednesday, August 31, 2022 8:50:37 PM

And a tremendous amount to be completed in short time.

I was impressed that you had two people I sincerely respect on the committee. Insights from the law enforcement and Homeland Security Department must not be ignored. They deal with this continuously and have deep expertise, if you can access it.

I have an extensive background in identity theft, identity impersonation, website hijacking, and various approaches to mitigation. I don't envy you addressing this challenge.

In a previous email I suggested that a new registrations should result in a snail mail to everyone whose name and address is provided because the process defined in the current legislation is "too little, too late." The process, as currently mandated, relies upon the impacted party to realize the theft and complain. Worse, the complaint process is not trivial. A snail mail immediately following registration may help. However, that mail must be very aggressive, notifying the recipient that their address had been used in a corporate registration and that, if they are not part of that corporation, there is a very real risk that they will be sucked into a legal nightmare. The mailing must include both a prepaid response postcard and a secure web link that they can use to either acknowledge or refute the legitimacy of the registration. I now realize that such an effort may be necessary but is not sufficient.

If nothing else, I would make the initial complaint process trivial!!! You want to encourage the complaint, not do the Attorney General's work for them.

Beyond that, I have one, overriding, suggestion for the committee: in the cybersecurity domain, we first define the threats (who, why, how) and then consider mitigations. You are facing multiple threats, and I suggest that you address each of them separately because the counteractions may be different.

During the call you mentioned the case where a new registration falsely uses an existing Colorado address. Separately, you mentioned the case where an existing registration is hijacked. Those are very different and require separate mitigations. There may be other use cases that weren't addressed; your law enforcement and Homeland Security participants should be able to identify them.

Because you are limited by existing funding and probable budget constraints, I would also suggest that you consider a staged remediation recommendation to the legislature. For example, it is possible to validate a residential name/address combination using data maintained by one of the three credit bureaus, but that requires an entire project to implement. And, this doesn't work for all registrations, specifically those where the corporation or registered agent is a business, but it's likely to identify the cases where the miscreants have chosen a random address. This is also the situation where a strongly worded (snail mail) letter, *using a vocabulary below the sixth grade level*, may be somewhat effective. Note that there are existing commercial databases that can separate business from residential addresses, allowing a more precise selection of remedial actions, but that's yet another IT project.

Registration hijacking is a very different threat and requires a different mitigation. This is a situation where it would be helpful, as one caller recommended, to perform a computer test of "similarity." This is more difficult than it might sound, and the software to do this well is expensive and requires continuous support and enhancement. A less strict approach, however, could be implemented with technologies similar to "soundex," i.e., sounds like. Recognizing a similarly, however, simply creates a new problem set, because a similar name could very well, and is likely to be, a legitimate registration. This is probably a situation where human review and followup may be required, which is expensive and labor-intensive. I would note, however, that this is commonly done with Internet domain registrations, so there is probably some technology available, if it can be identified.

I am concerned about the issue raised by one caller, which is the reality that SOS sells lists of Colorado corporate registrations. That's not a criticism. Colorado sells lists of automobile registrations, too, which is far more intrusive. I have deep experience in the consumer/business database aggregation world. I suspect that when you sell (rent) that data, it soon gets aggregated with many other datapoints and may well be a resource for those who wish to hijack a corporate name, reputation, etc. You may wish to examine the conditions under which that data is provided, possibly strengthen the constraints, drastically strengthen the penalties, and search for companies that can detect when that data has been misused.

I'm not current on the tactics used to identify and thwart identity theft, but I am aware that a significant amount of innovation is addressing that topic. You may wish to reach out, through your Homeland Security representative, for help from those who are engaged on the leading edge. I'm quite sure that knowledge has application in other State of Colorado departments, particularly those that provide aid to those in financial need. (And, yes, I have enough experience in government to understand how difficult it is to collaborate with other departments!)

Two closing points:

- During the call reference was made to some "secure" filing process offered by the SOS. Despite registering my corporation over twenty years ago, or perhaps because of that, I was unaware of this capability. I'll be looking into it tomorrow.
- Two callers mentioned multi-factor authentication. In today's online world, that's mandatory. It is not, however, easy to implement and too many users will be unable to understand their responsibility. I don't have a satisfactory recommendation to address that. However, I'm sure that the Secretary of State is just one of many parts of Colorado State and local government facing this requirement. The Federal government has yet to arrive at a reasonable MFA solution outside the Defense and Intell communities, but one is desperately needed. Privacy is a growing concern, and any government-managed MFA implementation is going to be highly suspect. This may be the most difficult problem to solve. I'd suggest it's beyond the committee's charter, but some agency in Colorado MUST accept this challenge.

Thank you for your dedicated work and your willingness to take on this challenge. I'm reminded that tackling a "tame" problem can make one rich and famous, while tackling a "wicked" problem only leads to mental illness :-) This is most definitely a wicked problem.

Rog

--
Roger Loeb

President & CEO
The MarTech Group, Inc.
4673 Moonshine Ridge Trail
134
[redacted]