Topic: Business Identity Theft

Question by: Paula Artzer

Jurisdiction: Kansas

Date: 27 October 2010

Jurisdiction	Question(s)
	1) Have you had issues with Business Identity Theft in your state or area of jurisdiction with regards to the information stored on your website? 2) If so, how have you addressed the issue, (i.e.: email notification of account activity, password protection, etc.)? 3) Has this approach been successful? 4) If you have not experienced issues as yet, are you taking a pro active stance to this type of crime? 5) What are your plans to address this issue? 6) If there is a website you have created for the public to address this issue, if so can you provide the web address? 7) Do you have a contact in your office we could speak with for further details if needed?
Manitoba	
Corporations Canada	Corporations Canada accepts online filings under the Canadian Business Corporations Act (CBCA) for annual report filings, changes to a corporation's registered office address and to its directors, as well as dissolutions. A filer must first provide a valid login credential, consisting of a six-digit access code referred to as a "Corporation Key". The Corporation Key is supplied to new corporations upon incorporation. A corporation can also request a new key or a replacement key at any time; any current key is then voided and a new key is sent by regular mail to the registered office of the corporation that Corporations Canada currently has on file. Alternatively, registered intermediary firms (such as law firms, accounting firms and search houses) who have been granted Registered Intermediary (R.I.) keys and who login using their R.I. valid keys, can file documents on behalf of their clients without the need to supply Corporation Keys. Other business corporation filings such as annual reports, amendments (e.g. the minimum or maximum number of directors) or continuance into the CBCA are subject to online payment of fees by credit card. These can be filed without login credentials.
Alabama	
Alaska	

Arizona	
Arkansas	
California	
Colorado	
Connecticut	
Delaware	
District of Columbia	
Florida	1. Have you had issues with Business Identity Theft in your state or area of jurisdiction with regards to the information stored on your website? Yes. There have been amendments or annual reports filed to change all officers/directors/managers/managing members and principal addresses. These appear to be done on companies with good credit scores to be used for their own personal gain. When the "real" owner discovers the "business identity theft" they seem to always blame it on the FEI# being available on our website. I believe that public availability of the FEI# will be an issue to be addressed in Florida soon. 2. If so, how have you addressed the issue, (i.e.: email notification of account activity, password protection, etc.)? We have no way of determining "business identity theft". It can occur with "paper filings" as well as "online filings". Our position is that it is a private matter to be resolved by the party(ies) harmed. 3. Has this approach been successful? N/A 4. If you have not experienced issues as yet, are you taking a pro active stance to this type of crime? There is no pro active position we can take. 5. What are your plans to address this issue? It's a "wait and see" situation, currently. 6. If there is a website you have created for the public to address this issue, if so can you provide the web address? N/A 7. Do you have a contact in your office we could speak with for further details if needed?
Georgia	
Hawaii	
Idaho	
Illinois	
Indiana	
Iowa	
Kansas	
Kentucky	
Louisiana	
Maine	
Maryland	
Massachusetts	
Michigan	
Minnesota	
Mississippi	

Missouri	
Montana	
Nebraska	
Nevada	
New Hampshire	New Hampshire has not seen much in the way of business identity theft. The few that we had were family issues and had to be dealt with in civil court
New Jersey	
New Mexico	
New York	
North Carolina	
North Dakota	While North Dakota's online utilities are still being developed with login and password protection, we did have some experience with corporate identity theft in the late 90's when nonprofit corporations were first administratively dissolved for failure to file annual reports. Many of those dissolved entities had long been abandoned but did have federal tax exemption. We have since adopted legislation that now requires any entity that has been dissolved for longer than one year to obtain a court order from the district court for reinstatement. This court order has been adopted in all of our business entity statutes. Since its adoption, we've not seen any further attempts to resurrect "dead" entities by unrelated parties.
Ohio	
Oklahoma	
Oregon	
Pennsylvania	
Rhode Island	
South Carolina	
South Dakota	
Tennessee	
Texas	
Utah	
Vermont	
Virginia	
Washington	1. Have you had issues with Business Identity Theft in your state or area of jurisdiction with regards to the information stored on your website? No, but we do not store any information on our website and display only public information. We have seen some hijacked certificates, but are not sure how those certificates were obtained. We do not display certificates on our web site. 2. If so, how have you addressed the issue, (i.e.: email notification of account activity, password protection, etc.)? 3. Has this approach been successful? 4. If you have not experienced issues as yet, are you taking a pro active stance to this type of crime? Somewhat – it's hard to address an issue that hasn't really happened yet. 5. What are your plans to address this issue? We plan to use Georgia's model of email alerts when a change is made to

	a corporation's documents. 6. If there is a website you have created for the public to address this issue, if so can you provide the web address? No 7. Do you have a contact in your office we could speak with for further details if needed? Just me, Pam
West Virginia	
Wisconsin	
Wyoming	

Additional comments:

NASS will be organizing a Business Identity Theft discussion group/task force next month. We will be happy to reach out to you to participate. We need to wait until after the elections though-we have a small staff here at NASS and we have planned to take on this major project after next week. I can tell you that CO (Sarah Steinbeck, Sarah.Steinbeck@SOS.STATE.CO.US) and GA (Vince Russo,vrusso@sos.ga.gov)have been very active in this arena. Also Cyndi Festa at Dun & Bradstreet (festac@dnb.com) is very knowledgeable on this issue and would be a great resource for you.

Full text of email:

Good Morning from Kansas! We are exploring opportunities to address the Business Identity Theft issues that are arising that can affect our offices. Since we store information on our websites for public access that can make a business vulnerable to this type of crime, we would like to know

1) Have you had issues with Business Identity Theft in your state or area of jurisdiction with regards to the information stored on your website?
2) If so, how have you addressed the issue, (i.e.: email notification of account activity, password protection, etc.)?
3) Has this approach been successful?
4) If you have not experienced issues as yet, are you taking a pro active stance to this type of crime?
5) What are your plans to address this issue?
6) If there is a website you have created for the public to address this issue, if so can you provide the web address?
7) Do you have a contact in your office we could speak with for further details if needed?

We really appreciate your input and assistance on this matter!

Thank you,

Paula

PAULA ARTZER
Business Analyst
Kansas Secretary of State
785-296-2908 P | 785-296-4570 F
Memorial Hall, 1st Floor | 120 SW 10th Ave. | Topeka, KS 66612-1594
www.kssos.org