Topic: Fraudulent Filings

Question by: Robert Lindsey

Jurisdiction: Virginia

Date: September 2, 2021

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
Manitoba	
Corporations Canada	
Alabama	
Alaska	

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
Arizona	
Arkansas	
California	
Colorado	
Connecticut	
Delaware	
District of Columbia	
Florida	
Georgia	
Hawaii	

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
Idaho	
Illinois	
Indiana	
Iowa	
Kansas	
Kentucky	
Louisiana	
Maine	
Maryland	
Massachusetts	

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
Michigan	
Minnesota	
Mississippi	
Missouri	
Montana	
Nebraska	
Nevada	
New Hampshire	
New Jersey	

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
New Mexico	
New York	

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
North Carolina	You have been busy if you have done everything on your list below recently. North Carolina has done everything on your list except move toward a dual factor authentication. I did participate on the Fraudulent Filing 411 Office Hours and ran the names and address provided on the summary through our system. NC doesn't have her names or addresses within our system. About a month ago a complaint came in from a company indicating someone filed an amened annual report making changes to their registered agent name, address, principal off mailing address and the company officials. When we did some investigation on the IP address and device used it brought about 42 similar filings, and on four other devices. However, more than one registered agent name was used. One such name used as the registered agent (the first) was Jonathan Smith. When I contacted all 43 entities to get the Business Registry data accurate, most of them also indicated that they had been contacted by Verizon and/or AT&T for mobile phone orders with the name of the registered agent used. They denied knowledge and the account was deemed fraudulent with Verizon and/or AT&T. We now have a complaint from Jonathan Smith indicating his name and address were used in the fraudulent filings. It also appears that complainant Jonathan Smith is former local law enforcement. Our investigative team is trying to determine the address where those mobile phones were to be delivered, to eventually identify the actual fraudster. I hope this narrative helps other states.

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
North Dakota	
Ohio	
Oklahoma	
Oregon	
Pennsylvania	
Rhode Island	
South Carolina	
South Dakota	
Tennessee	
Texas	

Jurisdiction	Question(s)
	As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail. Based on this particular filer we have done the following: * We added functionality to our system so we can quickly disable User accounts. (55 accounts to date) * We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model) * We have blocked numerous IP's * We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity * We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer * We had our payment provider shut down numerous credit card and echeck accounts. * We continue to work with our Network and Security Teams * We are working with law enforcement * We are pursuing dual factor authentication (Civix/Experian) * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass. * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again. Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!
Utah	
Vermont	
Virginia	
Washington	
West Virginia	
Wisconsin	
Wyoming	

Additional comments:

Full text of email:

As discussed in our "IACA Office Hours - Fraudulent Filings" meeting I would like to share and issue that we are currently experiencing in the Commonwealth of Virginia. For the folks who attended the call/meeting this may be a bit redundant but I would like to see if this filer is filing in other jurisdictions and ascertain the volume of filings she has filed. See attached for additional detail.

Based on this particular filer we have done the following:

* We added functionality to our system so we can quickly disable User accounts. (55 accounts to date)
* We added functionality to our system that will prevent someone from being able to setup an account through legitimate means. (Block name/address so she cannot move to the Experian Model)
* We have blocked numerous IP's
* We have blocked emails so this individuals would not be alerted to the fact that we have taken the appropriate action to unwind her activity
* We are running multiple queries daily to ensure we identify all filings associated filings to this particular filer
* We had our payment provider shut down numerous credit card and echeck accounts.
* We continue to work with our Network and Security Teams
* We are working with law enforcement
* We are pursuing dual factor authentication (Civix/Experian)
    * This will be on a point forward basis therefore this will not affect any of the existing accounts we currently have on file. To setup a new account you will have to enter your cell phone number and Experian will validate if that is a valid number associated to the name/address provided based on their data. If the numbers do not match this would be considered a fail if they do match a text would be sent to the cell phone and that code would have to be entered to move forward and would be deemed a pass.
        * It is worth pointing out that this is a one-time occurrence to setup the account. After the account is setup the customer/filer will not experience any dual factor authentication again.

Based on this particular filer/submitter filings we cannot determine what she is trying to accomplish or what the goal is for her to setup entities and file against other entities. I would like to hear what other jurisdictions think and what they are currently experiencing. In the call we did hear some interesting facts/scenarios that certain jurisdictions were experiencing and I hope they will share with the greater audience via the listserv. I'm also interested in everyone's thoughts on whether IACA needs another listserv for this subject matter, publish more material concerning fraudulent filings, a dedicated slot on IACA Conference Agenda etc. I appreciate that IACA initiated and hosted the call concerning fraudulent filings!

Thanks, Robert

Robert Lindsey | Assistant Deputy Clerk | Office of the Clerk

804-371-9424 (direct) | 804-370-2696 (cell) | robert.lindsey@scc.virginia.gov<mailto:robert.lindsey@scc.virginia.gov>

[SCC Logo Horizontal-blue color text]