Elad Gross, Attorney at Law
5653 Southwest Ave. 314-753-9033
St. Louis, Missouri 63139 elad.j.gross@gmail.com Licensed in Missouri

October 21, 2021

Office of the Missouri Governor
P.O. Box 720
Jefferson City, MO 65102
SENT VIA EMAIL TO ANDREW BAILEY AND BY CERTIFIED MAIL

Missouri Office of Administration
P.O. Box 809
Jefferson City, MO 65102
SENT VIA EMAIL TO COMOFC@OA.MO.GOV AND BY CERTIFIED MAIL

Missouri Department of Elementary and Secondary Education
P.O. Box 480
Jefferson City, MO 65102
SENT VIA EMAIL TO COMMISSIONER@DESE.MO.GOV AND BY CERTIFIED MAIL

Office of the Cole County Prosecutor
311 E. High Street, 3rd Floor
Jefferson City, MO 65101
SENT VIA EMAIL TO LOCKE THOMPSON AND BY CERTIFIED MAIL

Missouri State Highway Patrol
1510 East Elm Street
P.O. Box 568
Jefferson City, MO 65102
SENT VIA EMAIL TO DDCCMAIL@MSHP.DPS.MO.GOV AND BY CERTIFIED MAIL

Office of the Missouri Attorney General
207 W. High St.
P.O. Box 899
Jefferson City, MO 65102
SENT VIA EMAIL TO SUNSHINEREQUEST@AGO.MO.GOV AND BY CERTIFIED MAIL

Uniting Missouri PAC
P.O. Box 444
Farmington, MO 63640
SENT VIA EMAIL TO JHANCOCK@HANCOCKPROUTY.COM AND BY CERTIFIED MAIL

Victory Enterprises, Inc.
5200 SW 30th St.
Davenport, IA 52802
SENT VIA EMAIL TO INFO@VICTORYENTERPRISES.COM AND BY CERTIFIED MAIL

LITIGATION HOLD REQUEST AND DEMAND

Dear Missouri Office of the Governor Staff, Missouri Office of Administration Staff, Missouri Department of Elementary and Secondary Education Staff, Office of the Cole County Prosecutor Staff, Missouri State Highway Patrol Staff, Uniting Missouri PAC Staff, Victory Enterprises, Inc., Staff, Governor Mike Parson, Commissioner Margie Vandeven, John Hancock, and Charlotte Boyer,

This is a litigation hold request regarding all records and other physical evidence in your possession involving Professor Shaji Khan and any investigation into, discussion of, or publications made regarding the security flaw discovered on the Missouri Department of Elementary and Secondary Education website in October 2021.

Background

On or around October 11, 2021, Josh Renaud, a reporter with the St. Louis Post-Dispatch, asked Dr. Shaji Khan, a cybersecurity professor at the University of Missouri-St. Louis[1], to verify a potential major security flaw on a website for the Missouri Department of Elementary and Secondary Education. Mr. Renaud told Professor Khan that he had unexpectedly discovered the flaw. The public website permitted visitors to look up the credentials of Missouri

[1] Dr. Shaji Khan's UMSL page can be found online at https://www.umsl.edu/divisions/business/About%20the%20College/Faculty/Information%20Systems/khan.html. His CV – which includes his extensive service to the State of Missouri, elected officials, teachers, nonprofit organizations, the regional economy, and his students over his years as a professor – is also available online at http://www.umsl.edu/~khanshaj/cv_ShajiKhan.pdf.

teachers. Users could look up teachers by school assignments or by their last names and last four digits of their Social Security numbers. However, due to a major security flaw present in its design, the website was programmed to send the full Social Security number of Missouri teachers to every visitor to the website, whether the visitor was aware or not. That information was also programmed to be automatically stored in the visitors' web browsers. Professor Khan agreed to verify whether the security flaw existed only if Mr. Renaud agreed not to publish any story until the State of Missouri had an opportunity to protect teachers' sensitive information if a flaw was in fact present. Mr. Renaud agreed.

On October 11-12, 2021, Professor Khan verified the security flaw. He did so by:

- Visiting the public website, which was accessible by anyone and did not require a login;
- Looking at the publicly available source code, which can be easily done by anyone on any webpage under the "View" menu option;
- Identifying a suspicious piece of the source code referred to as "View State" that can contain security flaws like the one found here; and
- Translating the source code into plain text, which can also be done by anyone.

This entire process could be completed by anyone in a matter of just a few minutes. None of the data was encrypted, no passwords were required, and no steps were taken by the State of Missouri to protect the Social Security numbers of its teachers that the State automatically sent to every website visitor.

The View State security flaw verified by Dr. Khan has been well known in the field of cybersecurity for over a decade and should not be present on websites in 2021. *See* Bryan Sullivan, *Security Briefs – View State Security*, July 2010, available online at https://docs.microsoft.com/en-us/archive/msdn-magazine/2010/july/security-briefs-view-state-security; *see also* Troy Hunt, *How Not to "Hide" Sensitive Data in Plain Sight with View State*, May 14, 2014, available online at https://www.troyhunt.com/how-not-to-hide-sensitive-data-in-plain/. This security flaw has two simple solutions: One, encrypt the View State so it cannot be read by any member of the public, or two, do not put sensitive information like Social Security numbers in the View State. *See id.* The State of Missouri implemented neither solution. Instead, the website transmitted Social Security numbers to its visitors, whether those visitors

were aware or not. There is likely no way to tell how many teachers were compromised as a result of the State's actions.

On October 12, 2021, shortly after Professor Khan verified the security flaw, Mr. Renaud told Professor Khan that he had notified the Missouri Department of Elementary and Secondary Education. On or around October 13, 2021, after the Department took down the compromised website, the St. Louis Post-Dispatch published a story about the security flaw.

On October 13, Missouri Commissioner of Education Margie Vandeven published a statement regarding the security vulnerability. Commissioner Vandeven stated: "Through a multi-step process, an individual took the records of at least three educators, unencrypted the source code from the webpage, and viewed the social security number (SSN) of those specific educators." This statement was false. The State of Missouri transmitted Social Security numbers to every visitor to the website, and none of the source code for the website was encrypted. Because of the way the website was programmed, the State of Missouri saved teachers' Social Security numbers on every website visitor's web browser automatically. No one had to decrypt anything to see the Social Security numbers.[2] The Missouri Department of Elementary and

---

[2] Decoding and decryption are not the same process. Decoding and encoding are the simple processes of translating data into different formats. For example, binary data (0's and 1's) can be encoded into a sequence of printable text characters, and the textual representation can be decoded back into binary data. The process is often automated with encoders and decoders to meet data formatting requirements. The process can be broadly compared to language translation through services like Google translate.

Encryption is the transformation of data – plain text – into a form that conceals the data's original meaning to prevent it from being known or used - cipher text. Properly implemented encryption is designed to protect the confidentiality of sensitive data.

In this situation, sensitive data sent by the State's web application to every visitor's browser was merely translated into a different format – Base64 encoding – and translated back to readable text to identify the security flaw. Because the sensitive data was not encrypted or otherwise protected, and because the State of Missouri chose to transmit teachers' Social Security numbers through its publicly available website, any member of the public could easily see teachers' Social Security numbers by simply translating the data the State was sending to everyone.

Sensitive data should never be stored in the View State in the first place. View State is simply Base64 encoded and can easily be viewed by anyone because it is readily available in the browser. In the extreme case where sensitive data must be transmitted to the user's browser, the View State should be encrypted. The State's Credential Checker Application had no unavoidable need to store and send Social Security numbers in the View State. Despite that

Secondary Education republished Commissioner Vandeven's statement on its website.

On October 13, 2021, the Missouri Office of Administration issued a press release. In that press release, the Office of Administration stated that a "hacker" accessed the Social Security numbers of teachers. This characterization was also false. The State of Missouri automatically transmitted teacher Social Security numbers to every website visitor. No one who discovered and reported this security flaw attempted to gain unauthorized access to or "hack" the website.

On October 14, Missouri Governor Mike Parson made several public pronouncements, including by widely shared and transmitted video on the Governor's official Facebook page and publicly available written posts on both the Governor's official Facebook and Twitter accounts. In those statements, Governor Parson described the individuals who notified the state that it was illegally transmitting teachers' Social Security Numbers to every website visitor as "hackers." Governor Parson also promised to "bring to justice anyone who hacked our system and anyone who aided or encouraged them to do so in accordance with what Missouri law allows and requires." The Governor's characterization was also false. Additionally, Missouri law does not prohibit internet users from accessing public websites, and it does not prohibit internet users from looking at unencrypted, publicly available source code for web pages. Missouri Revised Statute § 610.035 does prohibit the government from transmitting Social Security numbers. However, the Governor did not mention any investigation he was conducting into government wrongdoing.

On October 15, 2021, a Missouri State Highway Patrol Trooper contacted Professor Khan and asked to interview him. The Trooper confirmed that the interview regarded statements Professor Khan had made to the St. Louis Post-Dispatch.

On October 19, 2021, Commissioner Vandeven provided a statement to the St. Louis Post-Dispatch shifting the blame from the State for the security vulnerability to those who discovered and responsibly reported it.

On October 20, 2021, an organization called Uniting Missouri PAC published a video on YouTube, Twitter, and Facebook calling for those involved

---

fact, it still did. To make matters worse, the data was not encrypted to protect the sensitive data. That created the major security flaw which was responsibly disclosed to the State.

in finding and responsibly reporting the website security flaw to be "brought to justice" and claiming that those who provided Missouri's teachers with an immense service "exploit[ed] private information." The video does not mention that the State of Missouri was the entity that exploited teachers' private information by transmitting their Social Security numbers to every visitor to its poorly designed public website. Uniting Missouri PAC is also actively using this defamatory video in two advertisements on Facebook, with one ad targeting 5,000-10,000 people in Missouri that has already been shown 2,000-3,000 times and one ad targeting 1,000-5,000 people in Missouri that has already been shown 1,000-2,000 times. Uniting Missouri PAC is a political action committee registered with the Missouri Ethics Commission. Its chairman is listed as John Hancock and its treasurer is Charlotte Boyer. The Facebook page is managed by Victory Enterprises, Inc., an organization that has an Iowa address. According to its website, Uniting Missouri PAC appears to support Missouri Governor Mike Parson exclusively.

Due to the actions of Governor Mike Parson, Commissioner Vandeven, the Missouri Office of Administration, the Missouri Department of Elementary and Secondary Education, the State of Missouri, and Uniting Missouri PAC, Professor Khan has suffered substantial harm. Professor Khan has had to hire legal counsel at his expense. He has also had to suspend discussing cybersecurity issues with members of the press, which was previously an important component of his effort to educate the public about data privacy and cybersecurity issues. He has been under intense stress as a result of the baseless investigation into him and the ongoing attack on his reputation and credibility. Professor Khan is a respected expert in his field who has repeatedly performed valuable services for the State of Missouri and its residents. The State, its officials, and their political operations have no grounds to defame and harass a private citizen who helped protect Missouri teachers.

Legal Analysis

No Probable Cause to Investigate Violation of RSMo. § 569.095 or 18 U.S.C. § 1030

The statute Governor Parson publicly claimed was violated was Missouri Revised Statute § 569.095. That statute states:

> 1. A person commits the offense of tampering with computer data if he or she knowingly and without

> authorization or without reasonable grounds to believe that he has such authorization:
>
> (1) Modifies or destroys data or programs residing or existing internal to a computer, computer system, or computer network; or
>
> (2) Modifies or destroys data or programs or supporting documentation residing or existing external to a computer, computer system, or computer network; or
>
> (3) Discloses or takes data, programs, or supporting documentation, residing or existing internal or external to a computer, computer system, or computer network; or
>
> (4) Discloses or takes a password, identifying code, personal identification number, or other confidential information about a computer system or network that is intended to or does control access to the computer system or network;
>
> (5) Accesses a computer, a computer system, or a computer network, and intentionally examines information about another person;
>
> (6) Receives, retains, uses, or discloses any data he knows or believes was obtained in violation of this subsection.
>
> 2. The offense of tampering with computer data is a class A misdemeanor, unless the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, the value of which is seven hundred fifty dollars or more, in which case it is a class E felony.

Under the cited statute, Professor Khan committed no crime. Every visitor to the Missouri Department of Elementary and Secondary Education's website with the security flaw received teachers' Social Security numbers and sensitive personal information unwittingly. The public website never indicated to any viewer that they did not have access to any part of the website. Data sent by the website was available in every visitor's browser in unencrypted form. Nothing on the website required a password to access. Professor Khan and every other visitor to the website had reasonable grounds to believe that they had authorization to view the unencrypted, unsecured, public website.

Courts interpreting a similar federal law also agree with this conclusion. The Computer Fraud and Abuse Act prohibits "access[ing] a computer without authorization or exceed[ing] authorized access." 18 U.S.C. § 1030. Where a "website is publicly available on the Internet, without requiring any login, password, or other individualized grant of access," a visitor collecting information from the website is not doing so without authorization or in excess of authorization. *See Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932-34 (E.D. Va. 2010). This is true even if the visitor "scrapes" the website by using an automated system to copy information from the site. *Id.* The United States Supreme Court recently looked at the definition of "authorized access" and determined that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021). The Court cautioned the government from trying to define authorized access expansively and turning "millions of otherwise law-abiding citizens [into] criminals." *Id.* at 1654-62. That is what the State of Missouri is appearing to do here: Criminalize anyone who visited a public website affected by a security flaw created by the government, and especially punish those who happen to have the knowledge required to notice and report the flaw. The expansive reading by the State would criminalize other common behavior, such as using Google to search for a celebrity without their permission. *See* RSMo. § 569.095.1(5) ("Accesses a computer, a computer system, or a computer network, and intentionally examines information about another person").

The State does not have probable cause to investigate Professor Khan.

Cause to Investigate State's Violation of RSMo. § 610.035

The only violation of the law was committed by the State of Missouri and its officials. First, the State of Missouri violated Missouri Revised Statute § 610.035. The statute states:

> No state entity shall publicly disclose any Social Security number of a living person unless such disclosure is permitted by federal law, federal regulation or state law or unless such disclosure is authorized by the holder of that Social Security number or unless such disclosure is for use in connection with any civil, criminal, administrative or arbitral proceeding in any federal, state or local court or agency

> or before any self-regulatory body, including the service of process, investigation in anticipation of litigation and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state or local court. Notwithstanding any other provision of law to the contrary, the disclosure of Social Security numbers of deceased persons shall be lawful, provided that the state agency disclosing the information knows of no reason why such disclosure would prove detrimental to the deceased individual's estate or harmful to the deceased individual's living relatives. For the purposes of this section, **"publicly disclose"** shall not include the use of any Social Security number by any state entity in the performance of any statutory or constitutional duty or power or the disclosure of any Social Security number to another state entity, political subdivision, agency of the federal government, agency of another state or any private person or entity acting on behalf of, or in cooperation with, a state entity. Any person or entity receiving a Social Security number from any entity shall be subject to the same confidentiality provisions as the disclosing entity. For purposes of this section, **"state entity"** means any state department, division, agency, bureau, board, commission, employee or any agent thereof. When responding to any requests for public information pursuant to this chapter, any costs incurred by any state entity complying with the provisions of this section may be charged to the requester of such information.

The State had no reason to send visitors to the Missouri Department of Elementary and Secondary Education's website sensitive information about each of its teachers. The government is absolutely prohibited from sharing Social Security numbers in these circumstances. The government, therefore, violated the law.

Cause to Investigate State's Violation of RSMo. § 407.1500

Second, the State of Missouri violated Missouri Revised Statute § 407.1500. The statute requires government officials to provide accurate

information to victims of data breaches. Here, the State of Missouri and its officials improperly published Social Security numbers of approximately 100,000 teachers online. Instead of informing teachers of the nature of their failure, Missouri officials chose to minimize the security flaw created by the State and publicly blame the individuals who responsibly reported the problem to the proper authorities. The government has a responsibility to follow the law and provide accurate information to the teachers it failed. It did not and still has not, and the government has therefore violated the law.

State Agencies and Officials Defamed Dr. Khan

Third, Governor Parson, Commissioner Vandeven, the Office of Administration, the Department of Elementary and Secondary Education, and other state officials violated Missouri law regarding defamation, both through slander and libel. Defamation requires publication of a defamatory statement that identifies or is made regarding the plaintiff, is false, is made negligently with respect to a private individual, and causes damage to the plaintiff. *See Overcast v. Billins Mut. Ins. Co.*, 11 S.W.3d 62, 70 (Mo. 2000) (en banc). The Governor disparaged Professor Khan's character through a widely viewed and shared video on the Governor's official Facebook page, and the Governor shared the video on his official Twitter account. The Governor also published several written social media posts disparaging Professor Khan. Commissioner Vandeven published a false statement disparaging Professor Khan and made additional comments to at least one reporter defaming him. The Office of Administration and the Department of Elementary and Secondary Education published defamatory statements publicly. Uniting Missouri PAC published a a defamatory video through multiple social media outlets. These false publications have damaged Professor Khan's reputation.

State Agencies and Officials Violated Dr. Khan's Right to Free Speech

Fourth, the State of Missouri has violated Professor Khan's right to free speech as protected by the United States and Missouri Constitutions (U.S. Const., Amd. 1; Mo. Const., Art. I, § 8). Missourians have a right to speak freely without the threat of government retaliation, especially when it comes to matters of public concern. The government's threat of prosecution would have a chilling effect on people of ordinary firmness and has had such an effect on Professor Khan. Professor Khan has already had to suspend his normal interactions with members of the press. Additionally, the government's retaliatory actions will deter other Missourians from assisting the State when

they uncover wrongdoing. The State's actions here are prohibited under the law.

State Agencies and Officials Would Undertake a Malicious Prosecution

Fifth, the state of Missouri, if it proceeds with its investigation into Professor Khan, would violate the prohibition on malicious prosecution. Malicious prosecution generally requires the commencement of prosecution, the instigation or continuation of the prosecution by the defendant, termination of the proceeding in the plaintiff's favor, a lack of probable cause for the prosecution, malice on the part of the defendant, and damage to the plaintiff. *See Edwards v. Gerstein*, 237 S.W.3d 580, 582 (Mo. 2007) (en banc); *Crow v. Crawford & Co.*, 259 S.W.3d 104, 114 (Mo. Ct. App. 2008).

All of those elements would be met here if this case proceeds. Professor Khan is likely to prevail on the merits of any case brought against him. No statute in Missouri or on the federal level prohibits members of the general public from viewing publicly available websites or viewing the website's unencrypted source code. No reasonable person would think they were unauthorized to view a publicly available website, its unencrypted source code, or any of the unencrypted translations of that source code. There is no probable cause to investigate Professor Khan, and instigation or continuation of any proceeding against him would therefore be prohibited.

Request for Investigation

We request an investigation into the State of Missouri, the Missouri Office of Administration, and the Missouri Department of Elementary and Secondary Education with respect to a violation of Missouri Revised Statute § 610.035. The law absolutely prohibits state entities from sharing Social Security numbers with narrow exceptions that do not apply in this case. The State of Missouri transmitted potentially 100,000 teachers' Social Security numbers to visitors to the Department of Elementary and Secondary Education's website. We request that the Missouri State Highway Patrol and the Cole County Prosecutor investigate.

Additionally, Missouri Revised Statute § 407.1500 requires the government to provide specific information to teachers impacted by the security breach created by the State of Missouri. The law does not permit the government to provide false information to those affected, as multiple government officials have done here. The Attorney General has the exclusive

authority to protect teachers under this statute from the improper acts of the government. We request that the Attorney General investigate the government agencies and officials involved.

Preservation Demand

This request for a litigation hold applies to any and all records, including but not limited to publications, writings, social media posts, videos, emails, text messages, messages sent via text-deleting apps, video recordings, audio recordings, time sheets, written records, notes, reports, phone messages, phone logs, analyses, photographs, database logs, programming scripts, websites, web application source code, and any other material. This request also applies to any physical evidence outside of such records, including computer systems. Failure to preserve these records and evidence could lead to legal sanctions.

You are required to ensure compliance with this litigation hold request, including ensuring that all involved staff members understand their obligations under the law.

If you have legal representation, please provide this litigation hold request to them. I can be reached any time at Elad.J.Gross@gmail.com and at 314-753-9033.

Additional Demands

As a result of the actions of the State of Missouri, the Missouri Office of Administration, the Missouri Department of Elementary and Secondary Education, Governor Mike Parson, Commissioner Margie Vandeven, and Uniting Missouri PAC, Professor Khan has suffered significant reputational damage and substantial stress, has had to suspend his normal community education efforts, and has had to undertake substantial costs to defend himself from a baseless investigation, including hiring legal counsel at his expense. These parties, in their attempt to shift blame from themselves for compromising teachers' Social Security numbers, have opened the State of Missouri to additional liability. Every day the parties fail to address their wrongdoing increases the liability and eventual cost to taxpayers. For these reasons, Professor Khan demands that:

- The State of Missouri immediately ceases its baseless investigation into Professor Khan;
- The parties compensate him for reasonable attorney's fees incurred in defending himself from the baseless accusations of the parties and for the immense stress and disruption the parties have caused him;

- The Missouri Office of Administration, the Missouri Department of Elementary and Secondary Education, Governor Mike Parson, Commissioner Margie Vandeven, and Uniting Missouri PAC release separate, detailed, and public statements apologizing to Professor Khan, to be shared on their respective websites, with Missouri and national press outlets, on social media sites, and to anyone the parties communicated their false accusations;
- Governor Mike Parson convenes and livestreams another press conference to apologize to Professor Khan, sharing and maintaining the video on the Governor's social media pages; and
- Uniting Missouri PAC publishes another video apologizing to Professor Khan and purchases advertisements to promote that video as the organization is currently doing with its defamatory and false video.

Professor Khan has provided an immense public service to the State of Missouri. This is not the first time. In 2016, Professor Khan assisted the Missouri Secretary of State in securing its website, a site which allowed Missourians to register to vote and start their own businesses, after he noticed a flaw. For that crucial service, Professor Khan received thanks from the State for reporting the vulnerability. Five years later, Professor Khan is now sadly the target of his government despite the service he has provided to Missouri's teachers.

Professor Khan helped drive the University of Missouri-St. Louis to be designated as a National Center of Academic Excellence in Cyber Defense Education by the National Security Agency and the Department of Homeland Security. He has trained numerous security professionals, provided expert commentary to the press in an effort to educate the public about the importance of cybersecurity, led professional development cybersecurity seminars for Missouri teachers, presented to state officials, assisted nonprofit organizations in developing better security protocols, and has led multiple initiatives to make Missouri a cybersecurity talent hub.

If the state proceeds with this baseless investigation against him, we will explore every avenue to address the wrongdoing in court.

Thank you for your cooperation and time. We look forward to hearing from you soon. You may contact me directly at Elad.J.Gross@gmail.com or at 314-753-9033.

Sincerely,

Elad Gross
Attorney at Law