SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

KAMYAR JAHANRAKHSHAN, also known as KAMYAR JAHAN RAKHSHAN; ANDY or ANDREW RAKHSHAN; ANDY or ANDREW KAMYAR (or KAMIAR or KAMIER) RAKHSHAN

NO. 3:16mj636-BK

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
JUL 29 2016
CLERK, U.S. DISTRICT COURT
By _____ Deputy

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief:

On or about January 24, 2015 and January 25, 2015, in the Dallas Division of the Northern District of Texas and elsewhere, defendant **KAMYAR JAHANRAKHSHAN, also known as KAMYAR JAHAN RAKHSHAN; ANDY or ANDREW RAKHSHAN; ANDY or ANDREW KAMYAR (or KAMIAR or KAMIER) RAKHSHAN** knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer; in that the defendant knowingly caused a denial of service attack on the website Leagle.com, and by said transmission caused a loss aggregating at least $5,000 or more during a one-year period.

In violation of 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(c)(4)(A)(i)(I) and (B).

This criminal complaint is based on the facts set out in the attached affidavit.

Matthew R. Dosher
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence in Dallas, Texas, on July 29, 2016

RENÉE HARRIS TOLIVER
UNITED STATES MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF
A CRIMINAL COMPLAINT

I, **Special Agent Matthew R. Dosher**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of Criminal Complaint setting out probable cause to believe that defendant **Kamyar Jahanrakhshan,** also known as **Kamyar Jahan Rakhshan,**[1] **Andy** or **Andrew Rakhshan**, **Andy** or **Andrew Kamyar (or Kamiar or Kamier) Rakhshan** date of birth xx/xx/1979, has committed a violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B) (transmission of a code or command and intentionally causing damage to a computer). Although the criminal complaint only alleges the above violation, this affidavit sets out some additional facts revealing violations of 18 U.S.C. §§ 1030(a)(7)(A) (1030(c)(3)(A)) (extortion by threats to cause damage to a computer); 1030(b) (conspiracy to violate § 1030(a)); and 2261A (cyber stalking).

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since July 06, 2010. I have a Bachelor's of Science degree in Mathematics and prior to my employment by the FBI, I worked as a Production Enhancement Engineer and Pipeline Engineer for a large oil and gas services company. Since April 2014, I have been assigned to investigate violations of Federal law involving computer/technology crime including malicious activity, computer intrusions, and internet related fraud.

[1] In this affidavit, the references to **Jahanrakhshan** or **Rakhshan** refer to the same person.

During my employment, I have received training in such investigations through seminars, classes, official FBI training, and work related investigations. As a Federal Agent, I am charged with conducting investigations into violations of United States laws and given authority to execute warrants issued under United States authority.

3. In setting out the below facts, Affiant relies on the review of records from victims, law enforcement, and providers such as Google, Inc. and Yahoo!, Inc. Affiant also relies on information received from investigations conducted by other law enforcement agencies, domestic and foreign.

4. This affidavit merely is intended to provide an overview of the defendant's criminal conduct and more specifically, that there is sufficient probable cause for the issuance of a Criminal Complaint and a warrant for the arrest of **Kamyar Jahanrakhshan,** also known as **Kamyar Jahan Rakhshan, Andy** or **Andrew Rakhshan, Andy** or **Andrew Kamyar (or Kamiar** or **Kamier) Rakhshan**. This affidavit does not set forth all of Affiant's knowledge about this matter or regarding **Rakhshan**'s harassment of other victims.

STATUTES

5. The Criminal Complaint only alleges a violation of 18 U.S.C. § 1030(a)(5)(A). Section 1030(a)(5)(A) makes it a federal felony offense if an individual "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." Pursuant to 18 U.S.C. § 1030(c)(4)(B), said offense is punishable by a fine or imprisonment for not more than ten years, or both,

because the "loss to 1 or more persons during any 1-year period "was at least $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

6. The additional facts provided herein reveal violations of the following statutes:

a. 18 U.S.C. § 1030(a)(7)(A) makes it a federal felony offense if an individual "with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer." Pursuant to 18 U.S.C. § 1030(c)(3)(A), said offense is punishable by a fine or imprisonment for not more than five years, or both.

b. 18 U.S.C. § 1030(b) makes it a federal offense if an individual "conspires to commit or attempts to commit an offense under subsection (a) of this section."

c. 18 U.S.C. § 2261A makes it a federal felony offense if an individual "with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that (A) places that person in reasonable fear of the death of or serious bodily injury to a person; or (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person, said offense is punishable by a fine and imprisonment for not more than five years.

DEFINITIONS

7. A "protected computer" means a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

8. A denial of service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

9. A distributed denial of service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.

10. A botnet is a network of compromised computers programmed to receive commands without the owners' knowledge.

11. URL is a Uniform Resource Locater, which is an Internet Protocol address identifying or linking to a particular file on the Internet. The address usually begins with http and concludes with the domain name.

BACKGROUND – KAMYAR JAHANRAKHSHAN

12. **Jahanrakhshan** is 32 years old male born in Iran. In approximately 1991, **Jahanrakhshan** emigrated to the United States of America and became a USA citizen. In approximately 1995, he moved to British Columbia and obtained permanent resident status in Canada. **Jahanrakhshan**'s 2005 conviction for theft in the second degree from

the State of Washington: *The State of Washington v. Andrew Kamiar Rakhshan, aka: Kamyar Jarakhshan, Kamyar Jahanrakhshan*, File No. 03-1-01437-3, was vacated on August 4, 2011. **Jahanrakhshan** has a 2011 conviction for Fraud and Obstruction in Canada. He was sentenced and was incarcerated for approximately 18 months.

13. Due to the conviction, **Jahanrakhshan** was deported from Canada to the United States in or about September 2014.

PROBABLE CAUSE

A. LEAGLE.COM

14. In February 2015, a distributed denial of service (DDoS) attack on Leagle.com[2] was brought to the attention of FBI Dallas. The Leagle.com site is hosted at SoftLayer, a Northern District of Texas, Dallas Division based hosting company. According to information provided by the Leagle.com, it was contacted on or about December 30, 2014, by **Andrew Rakhshan** from the e-mail address andyrak@shaw.ca. This contact requested that a URL linking to a court decision involving **Rakhshan** be deleted. Claiming that he was the plaintiff in the case mentioned, **Rakhshan** stated that he did not want the opinion available on the internet as it was tarnishing his reputation and violating his privacy. **Rakhshan** offered to pay an administrative fee to have the post removed. Specifically, the facts are as follows:

a. Between on or about December 30, 2014 and on or about January 1, 2015, DJ at Leagle.com received e-mails signed by "**Andrew Rakhshan**" from the e-

[2] Leagle, Inc. is an aggregator of case law from Federal and certain State courts. The information is assessable at leagle.com.

mail address andyrak@shaw.ca. **Rakhshan** stated that a link hosted by the site Leagle.com was capable of tarnishing **Rakhshan**'s reputation and **Rakhshan** claimed this was a violation of his privacy. This link contained a court opinion in which **Rakhshan** was the plaintiff. **Rakhshan** offered to pay Johnson and Leagle.com for the removal.

b. Again on or about January 1, 2015, **Rakhshan** sent an e-mail to DJ from andrew.rakhshan@gmail.com[3] and offered to send DJ a $100 USD bill in a "Happy New Year" card for the removal of the five occurrences of "Andrew," the single occurrence of "Kamier," and **Rakhshan**'s home address from the opinion. **Rakhshan** also offered to send the $100 USD via PayPal.

c. On or about January 16, 2015, at 3:43:50 PM CST, **Rakhshan** sent an e-mail to DJ from andrew.rakhshan@gmail.com and requested DJ's fax number in order to send DJ an undisclosed item. Afterwards, **Rakhshan** claimed that the court opinion concerned a criminal matter for which he was found guilty, though he denied his guilt. **Rakhshan** once again requested that his first name, middle name, and home address be redacted. He then demanded an explanation why Leagle.com would not comply and offered the $100 USD again. The e-mail "I DESERVE AN EXPLANIATION NOW" was signed "**Andrew Rakhshan.**"

[3] Per Google Inc. records, the subscriber for andrew.rakhshan@gmail.com is Andrew Rakhshan. The account was created on 2014/10/18, and the alternate e-mails are andrew.rakhshan@gmail.com and akr9@sfu.ca..

d. On or about January 24, 2015 at 7:28 PM, **Rakhshan** sent an e-mail to DJ from andrew.rakhshan@gmail.com, claiming that he met a "group of hackers online whom are willing to launch a massive cyber attack on [leagle.com]." **Rakhshan** claimed that he had no other options to resolve the matter. He threatened to use these hackers to conduct a DDoS attack to force Leagle.com to comply with his demands. The e-mail was once again signed by "**Andrew Rakhshan.**"

e. On or about January 25, 2015, DJ and Leagle.com received the following message from "Anonymous Hackers <assn_drp@yahoo.com[4]>:"

We are the anonymous hackers group. This evening we launched a Distributed Denial of Service (DDoS) attack on your website Leagle.com.
We did that for free on behalf of Mr. Andrew Rakhshan who is being unjustly victimised by you. He has been profusely suffering for the past month because of your refusal to delete the following case law:
http://leagle.com/decision/In%20WACO%2020090427897/
If you do not remove it immediately, more severe attacks will hit your website in the coming days and weeks, and your users will be deprived of your service.
Be wise.

A copy of the court opinion accessed by said link is attached as Exhibit 1.

f. The Leagle.com site was hosted at the Northern District of Texas, Dallas Division based Internet hosting company SoftLayer. SoftLayer provided an analysis of the January 24, 2015, traffic to the Leagle.com site to FBI Dallas.

[4] Per Yahoo! Inc. records, the subscriber for assn_drp@yahoo.ca is JB, with a recovery email of vancouver4985@gmail.com. However, from his review of Rakhshan's e-mail accounts, Affiant has probable cause to believe that Rakhshan created and used the assn_drp@yahoo.ca e-mail account. Rakhshan discusses creating and using the assn-drp@yahoo.ca e-mail account and uses the vancouver4985@gmail.com e-mail account as recovery account for andyfromcanada@gmail.com (see footnote 6).

SoftLayer reported that between 8 AM and 4 PM a large amount of traffic targeted the IP address for Leagle.com. According to SoftLayer, the actions SoftLayer took could not mitigate the attack traffic. The DDoS attack subsided at approximately 4 PM on or about January 25, 2015.

g. According to Leagle.com, the company removed the link to the court opinion during the day but prior to 4 PM on or about January 25, 2015. Affiant believes that the DDoS attack subsided as a result of Leagle.com removing the link. Leagle.com estimated that time and resources allocated to the issue exceeded $10,000.00USD.

B. FAIRFAX MEDIA / THE SYDNEY MORNING HERALD

15. In or about April 2015, a DDoS attack on Fairfax Media[5] was brought to the attention of FBI Dallas. The Fairfax Media site is hosted at Quadranet, whose servers for this client were located in California. Between January 2015 and August 2015 (though not limited to that date range), **Rakhshan** communicated with DG of Fairfax Media by e-mail. Initially, **Rakhshan** requested that two articles from September 2011 posted on www.smh.com.au (The Sydney Morning Herald) be taken down from the site. After being informed that Fairfax Media would not be removing the articles, **Rakhshan** offered to send $500 AUD for the removal. Calling it a "generous offer" and a "donation," **Rakhshan** continued to claim that the lack of responses from DG meant that he was open to the offer.

[5] Fairfax Media is a media company in Australia and New Zealand.

16. On June 9, 2015, **Rakhshan** confirmed that DG had received the $500AUD. **Rakhshan** began e-mailing anyone connected with DG at Fairfax Media, requesting information on the money that was sent, and requesting the return of the money if the articles were not removed. **Rakhshan**'s e-mails became more combative. **Rakhshan** requested that the money "owed" to Rakhshan be sent by DG or Fairfax Media to JM in Vancouver, British Columbia. Throughout July 2015, **Rakhshan** continued to harass DG over the money, and accused DG of lying and stealing the money.

17. On or about February 16, 2015, Fairfax Media received an e-mail purporting to be from the "Anonymous Hackers" using the assn_drp@yahoo.ca e-mail address. In this e-mail, the "Anonymous Hackers" claimed responsibility for the DDoS attacks on Fairfax Media. Affiant's review of the andyfromcanada@gmail.com[6] account revealed that andyfromcanada@gmail.com received a blind cover copy of that e-mail. The "Anonymous Hackers" claimed that the attacks had been ongoing for the previous eleven days and would continue if the articles **Rakhshan** requested removed were not taken down. The substance of the e-mail to Fairfax Media follows:

> *"We are responsible for all of the DDoS attacks incurred by many of the Fairfax Media websites during the past 11 days. You must be aware of them*
>
> *Our demand to halt these attacks is simple and trivial.*
>
> *There are two articles that were published in one of your newspaper in 2011. They are concerning one of our colleagues."*

[6] Per Google Inc. records, the subscriber for andyfromcanada@gmail.com is Andy Rak. The account was created on 2007/08/11, and the recovery e-mail is vancouver4985@yahoo.com.

We are demanding their immediate Take Down. If you refuse, a systematic DDoS attacks against Fairfax Media websites will ensue. On the other hand, if you comply and delete the subject articles from your archives, all attacks will be immediately halted.

If you decided to comply, simply reply to this email and we will send you the subject URLs for deletion.

18. In or about September 2015, the Australian Federal Police informed FBI Dallas that **Rakhshan** had escalated his threats from DDoS attacks to faxes threatening bomb attacks. Through faxes, **Rakhshan** threatened to "call in bomb threats to different places including Courthouses in Vancouver."

19. As of October 8, 2015, **Rakhshan** sent e-mails to Fairfax Media from the andyfromcanada@gmail.com address claiming that he (**Rakhshan**) was entitled to a return of his money and he would continue to e-mail any Fairfax Media account he had until the money was returned.

20. In February 2016, The Sydney Morning Herald (smh.com) was the victim of a DDoS attack orchestrated by **Rakhshan**. The attacked smh.com server was hosted in the United States. On or about February 3, 2016, The Sydney Morning Herald received an e-mail purportedly from the "Anonymous Hackers" using the e-mail unix@fairfaxdigital.com.au, claiming responsibility for the DDoS attack on smh.com. Though the e-mail was sent from AU-Unix-Group, the full header information revealed that the original sender of the e-mail was the known assn_drp@yahoo.ca account.

21. On February 23, 2016, assn_drp@yahoo.ca sent an e-mail to The Sydney Morning Herald with the subject line "SMH Digital is DOWN again!!!" stating that if the

takedown demands were not met the attacks would not cease. The substance of the e-mail follows:

Hi Guys,
We just took down the SMH Digital once again. Your paying customers cannot login to read the SMH or other fairfax digital papers.
You know what to do to restore service. TAKE THESE DOWN:
http://www.smh.com.au/business/conman-hit-three-australian-banks-in-credit-card-sting-20110907-1jxr4.html
http://www.smh.com.au/business/canadian-conman-taps-banks-20110907-1jxtj.html
http://www.bordermail.com.au/story/934572/canadian-conman-taps-banks/

We wont stop our exploits against fairfax until these articles are removed.
Cheers,
Anonymous Hackers

Copies of the linked articles are attached as Exhibits 2, 3, and 4, respectively.

22. On February 25, 2016, assn_drp@yahoo.ca sent an e-mail to Fairfax Media with the subject line "ALL Fairfax Media Digital Editions are DOWN" stating that if the takedown demands were not met the attacks would not cease. The substance of the e-mail follows:

Good morning,

All of the Fairfax Media Digital News Paper Editions, including SMH are once again DOWN and inaccessible to your paying subscribers!
As promised before, we will abort ALL attacks and exploits again Fairfax Media, and will cease and desist forever, the minute you take down the following articles:
http://www.smh.com.au/business/conman-hit-three-australian-banks-in-credit-card-sting-20110907-1jxr4.html
http://www.smh.com.au/business/canadian-conman-taps-banks-20110907-1jxtj.html

Otherwise, the same trend will continue throughout the weekend....and in the coming days and weeks.

Cheers,Anonymous Hackers

C. METRONEWS.CA[7]

23. In 2014, **Rakhshan** exchanged e-mails with a representative of Metronews.ca. **Rakhshan** demanded that Metronews.ca delete articles involving **Rakhshan** from its site. To encourage Metronews.ca's compliance with **Rakhshan**'s demand, **Rakhshan** sent money to Metronews.ca. On January 2, 2015, **Rakhshan** sent the following e-mail from kjahanrakhshan@gmail.com to Metronews.ca.

> *Well, since you guesses my true identity correctly, I'll make my intentions more clear to you.*
> *When I was released from prison, I was deported from Canada. I now live in a non-extraditable country. I had someone mail that envelope to you. Since I have been deported from Canada and have been banned from entering it for LIFE, I want it out of my life. I cannot afford to be haunted and followed by this ordeal wherever I go in the world.*
>
> *If you do not comply with my demand, Metronews.ca will be hit with a massive cyber attack (DDOS). If you think that is a joke, just wait and see. As the article suggests, I am a 'sophisticated international fraudster'. It should be a fair inference that I am also a 'sophisticated cyber criminal'. Is that fair?*
>
> *I will utilize several criminal botnets to attack your webserver with thousands of hijacked IP addresses from around the world, and cause your server to crash due to memory exhaustion. That is a similar attack that was recently done on Toronto Police Department and Supreme Court of Canada Websites which caused them to be inaccessible to public for days.*
>
> *If cyber attacks (DDOS) still does not change your mind, then I will send death/bomb threats to Metro Offices across Canada and to their employees. I will continue this trend for as long as necessary until you succumb and press "delete". Again, since I have been banned from Canada for LIFE....I have NOTHING to lose!!!*

[7] Metro News is a daily newspaper brand available through traditional newsprint and online.

Now you can either call the North Vancouver RCMP (whom own all my files) at 604-985-1311 and let them laugh at you and tell you that "you are on your own..."; or just click the "delete" button. Which one will you choose [redacted]?

Regards,
Kamyar Jahanrakhshan

24. On January 6, 2015, **Rakhshan** sent the following e-mail from kjahanrakhshan@gmail.com to Metronews.ca:

What an idiot you are [redacted]? Still hasn't taken this shit down????
Well, say hello to your IT security manager and tell him you are gonna be hit with a 65Gbps of traffic this week.

I'll contact you again after the attack to see if you would reconsider the deletion request!

Regards,
Kamyar Jahanrakhshan

25. In late January 2015, **Rakhshan** sent several e-mails from kjahanrakhshan@gmail.com to Metronews.ca, advising that not only will he attack metronews.ca, he will begin attacking its advertisers.

26. On June 1, 2015, **Rakhshan** sent the following e-mail from kjahanrakhshan@gmail.com to Metronews.ca:

Listen you Bastards:
I have been peacefully negotiating with you for EXACTLY 3 months to NO avail.
I have not attacked ANY of your clients for the past three month.
THE GAME IS OVER. THIS IS YOUR ULTIMATUM:
You have until tomorrow Tuesday June 2nd, Noon Toronto Time, to take down my article, OR ELSE:
I will launch a massive cyber attack against one of your most prominent client.

Further, I will repeatedly harass and threat that client to STOP advertising with Metro, or else I will attack other sources in which they have advertising agreement with.

I will then do the same with ALL your big clients on a weekly basis.....

SO WAKE THE FUCK UP NOW AND DELETE THIS ARTICLE - OR GET READY FOR A REALLLLL WAR:

Metronews.ca/news/Vancouver/654274

Kamyar Jahanrakhshan

D. CBC.CA[8]

27. In 2014, **Rakhshan** exchanged e-mails with a representative of cbc.ca. **Rakhshan** demanded that cbc.ca delete articles involving **Rakhshan** from its site. To encourage cbc.ca's compliance with **Rakhshan**'s demand, **Rakhshan** sent money to cbc.ca. On January 6, 2015, **Rakhshan** sent the following e-mails from kjahanrakhshan@gmail.com to representatives at cbc.ca:

E-MAIL #1: *If you do not comply with my request and delete, I will keep attacking CBC.ca with a huge criminal botnet and tens of thousands of hijacked IP addresses. I will organize a massive cyber attack and take down CBC.ca, or at least cause some serious damage to your webserver by exhausting its memory capacity and making it unavailable to legitimate users (DDoS). Take note that your own editor has described me as a "sophisticated international fraudster". Isn't fair to say that I can also be a "sophisticated cyber criminal"?*
If cyber attacks still doesn't force you to implement my demand, then I will make death threats and bomb threats to your offices and employees across Canada; to all level from Editors to CEOs and their families. I wont stop until the article is deleted, even if it takes months.

E-MAIL #2: *FYI, CBC.ca will be hit by a 65 Gbps attack next week if you refuse deletion.*

[8] CBC stands for the Canadian Broadcasting Corporation.

28. On January 24, 2015, **Rakhshan** sent the following e-mail from kjahanrakhshan@gmail.com to a representative at cbc.ca:

> *I have been deported from Canada, and am trying to build a new life half a world away, but this nasty article of yours is taunting me every day.*
> *If you are skeptical of my deportation, a simple phone call to CBSA will affirm it. I have been banned from entering Canada for LIFE, and yet the Canadian Society are following me worldwide thru CBC, their largest news agency. THAT MUST END NOW.*
>
> *If you do not delete within the next 7 days, I will start making death and bomb threats against numerous CBC compounds across Canada. I will also threat the lives of CBC employees and their family. I live in a non-extraditable country, so have fun calling the Police.*
>
> *I have already sent my above intentions to several CBC email addresses, including [redacted] and [redacted]; but to no avail. I did not even receive a reply. This email will be my FINAL normal correspondence to CBC.*
>
> *I'll leave this in your hands.*
>
> *Kamyar Jahanrakhshan*

29. On January 30, 2015, **Rakhshan** sent an e-mail from andyfromcanada@gmail.com to tankshu04@gmail.com[9] with the subject line stating "HOLLY SHIT I JUST TOOK DOWN CBC.CA." **Rakhshan** included a screen shot of

[9] Affiant believes Tankshu04@gmail.com was used by a person that identified himself as MD. Affiant believes that MD hosted the server used by Rakhshan. In response to the "Holly Shit" e-mail, MD responded to Rakhshan, stating "[y]ou need to cool it with the spam attacking which I told you about before you bought a stresser login b/c you kill the service for everyone b/c every attack you run is on the same ips and it's always 800 seconds without stopping and you can't do that." "Yes when you're attacking with spam you take away from other users and you're abusing bandwidth on the servers which is why the tos say no spamming;" Affiant believes "tos" stands for terms of service.

a DDoS attack in the e-mail. On the same day, **Rakhshan** sent the following e-mail from kjahanrakhshan@gmail.com to a representative at cbc.ca:

> *If you fail to comply, I will attack you with much larger DDoS attacks. For tonight's attack I used a bandwidth of 10 TB (tetra bytes). I could acquire servers of up to 100 TB; meaning an attack 10 times larger than what I did tonight (your time zone off course)!*
> *Again I live in a non-extraditable country, so don't waste your time calling the Police! You will be hit with more attacks next week if I don't see a deletion. Next time I'll do it during your business hours. After all, I don't think I need to make bomb threats to CBC to get this deletion done!*
>
> *Regards,*
> *Kamyar Jahanrakhshan*

30. On April 28, 2015, **Rakhshan** sent the following e-mail from kjahanrakhshan@gmail.com to a representative at cbc.ca:

> *In addition, I will threat the lives of CBC employee all over Canada, from Atlantic to Pacific regions. Not only that, I will also threat the lives of families of CBC employees, whether they are children in school or senior citizens in nursing homes. I will also disrupt CBC offices too.*

31. On June 8, 2015, **Rakhshan** sent e-mails from kjahanrakhshan@gmail.com to representatives at cbc.ca, claiming responsibility for an attack on Radio Canada. On July 12, 2015, **Rakhshan** sent e-mails from kjahanrakhshan@gmail.com to representatives at cbc.ca, threatening to call in bomb threats to CBC across Canada.

E. CANADA.CA[10]

32. In 2014, **Rakhshan** exchanged e-mails with a representative of Canada.ca. **Rakhshan** demanded that Canada.ca delete articles involving **Rakhshan** from its site.

[10] Canada.com is a social media discussion site owned and operated by Postmedia Network Inc., a publisher of daily newspapers through traditional newsprint and online.

To encourage Canada.ca's compliance with **Rakhshan**'s demand, **Rakhshan** offered to send money to Canada.ca. On January 3, 2015, **Rakhshan** sent the following e-mails from kjahanrakhshan@gmail.com to representatives at postmedia:

> *If you do not comply with my request, I will keep attacking you with a huge criminal botnet and thousands of hijacked IP addresses. I will organize a massive cyber attack. I will eventually cause one of your many websites to crash, if not cause some serious damage to your webserver by exhausting its memory capacity and making it unavailable to legitimate users (DDoS). Take note that your own editors above have named me a "sophisticated international fraudster". Isn't fair to say that I can also be a "sophisticated cyber criminal"?*
>
> *If cyber attacks still doesn't force you to implement my above demands, then I will make death threats and bomb threats to your offices and employees across Canada; to all level from Editors to CEOs and their families. I will not stop until no remnant of "Jahanrakhshan" remains in Postmedia Network.*

33. On January 8, 2015, **Rakhshan** sent the following e-mails from kjahanrakhshan@gmail.com to representatives at postmedia:

> *I am still getting ready for that massive attack on Canada.com. That requires HUGE botnet and so it takes time to prepare it.*
>
> *But for now I am attacking one of your beloved and favorite clients: Inspiration Furniture:*
>
> *www.inspirationfurniture.ca*
>
> *You would have problem visiting that site today!!!! As you know their banner is on top of the Canada.com*
>
> *Should I call them and embarrass you all by telling them its ALL Postmedia's fault that your site in down?"*

34. From January 14, 2015 through January 24, 2015, **Rakhshan** continued to email representatives of Postmedia and Inspiration Furniture about deleting the articles, saying that the DDoS attacks would continue.

REQUEST FOR SEALING

35. I further request that the Court order that the Criminal Complaint, the Affidavit, and the arrest warrant, be sealed, except as necessary to facilitate the execution of the arrest warrant, until further order of the Court. These documents discuss an ongoing criminal investigation wherein the government is still collecting evidence. Accordingly, there is good cause to seal these documents because their premature disclosure may give the defendant and any accomplices an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Matthew R. Dosher
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on July 29, 2016

RENEE HARRIS TOLIVER
UNITED STATES MAGISTRATE JUDGE

RAKHSHAN v. WHATCOM COUNTY *NO. 61697-8-I*

ANDREW KAMIER RAKHSHAN, Appellant, v. WHATCOM COUNTY, Respondent.
Court of Appeals of Washington, Division One.
Filed: April 27, 2009.

Counsel for Appellant(s), Andrew Rakhshan (Appearing Pro Se), 3105 1077 West Cordova, Vancouver, BC, V6C2C6.
Counsel for Respondent(s), Randall Joseph Watts, Attorney at Law, County Courthouse Floor 2, 311 Grand Ave, Bellingham, WA, 98225-4048.

UNPUBLISHED

COX, J.

A thief has no right to possess stolen property.[1] Here, because the evidence submitted in opposition to Whatcom County's motion for summary judgment is "too incredible to be believed," Andrew Rakhshan has failed in his burden to show there are any genuine issues of material fact.[2] Whatcom County is entitled to judgment as a matter of law. We affirm the dismissal with prejudice and impose sanctions against Rakhshan.

In November 2003, the Whatcom County Sherriff seized five vehicles from a storage yard in Whatcom County based on the claim that Rakhshan had no right to possess the cars because he obtained them by using fraudulent credit cards. In June 2005, he commenced this conversion action against the County.

In 2005, following unsuccessful cross-motions for summary judgment by the parties, Whatcom County obtained authorization from the trial court for depositions in France pursuant to CR 28(b). The trial court sent a letter of request for international judicial assistance to the French court listing the witnesses to be examined and describing the evidence requested. The list included Rakhshan's relatives, Jean-Pierre Fournier and Francois Dupont, whom he had identified as persons with knowledge of the transactions at issue in acquisition of the cars the County seized. The Higher Level Court of Paris convened an International Rogatory Commission and took testimony from the County's witnesses. Neither Rakhshan's relatives nor Fournier nor Dupont appeared before the Commission. Moreover, Rakhshan failed to submit any questions to the Commission for examination of the witnesses.

Rakhshan then sought the trial court's permission to take depositions of his relatives in London and to present the deposition of Fournier, which Rakhshan alleged that he had taken while Fournier was recently in Canada. The trial court denied Rakhshan's motion and granted the County's motion to strike the Fournier deposition.

In December 2007, Whatcom County moved for summary judgment and requested an award of terms under CR 56(g). Rakhshan responded, and the trial court granted the County's motion, dismissing the complaint with prejudice. Thereafter, the court also denied Rakhshan's post-hearing motion to strike evidence submitted on behalf of the County in support of its motion for summary judgment. The court also awarded Whatcom County a judgment of $27,103.79 against Rakhshan for attorney fees and expenses. The judgment was supported by findings of fact and conclusions of law in support of the fee award under CR 56(g) and CR 11.

Rakhshan appeals.

DISCOVERY AND EVIDENTIARY RULINGS

Rakhshan argues that the trial court abused its discretion in the management of discovery and in the consideration of evidence. Regarding discovery, Rakhshan contends that the trial court erred by allowing the Rogatory Commission's examination of the French witnesses, striking the deposition of Fournier, and granting the County's motion for a protective order prohibiting the depositions of Rakhshan's relatives. He complains that the use of the French procedure prevented him from cross-examining the witnesses and the trial court's refusal to allow him to make alternative arrangements to depose his witnesses improperly prevented him from presenting his evidence. We disagree.

We will not disturb the trial court's rulings on discovery matters absent an abuse of discretion which caused prejudice to a party.[3]

Exhibit 1

On June 15, 2007, the trial court denied Rakhshan's motion to prohibit the examination of the French witnesses, but ordered that he had the "responsibility to follow the process required by French law" to exercise his right to cross-examine the French witnesses. At a hearing on October 26, 2007, Rakhshan admitted that he never sent any questions to the French Rogatory Commission. Because Rakhshan failed to exercise the right to cross-examination specifically provided by the trial court, he fails to establish any abuse of discretion causing prejudice.

Similarly, Rakhshan cannot demonstrate any abuse of discretion in the trial court's decision to prohibit additional depositions of Rakhshan's relatives in England and to strike the Fournier deposition. In its letter of request to the French court, the trial court listed Rakhshan's relatives, Dupont and Fournier, along with the addresses for each as provided by Rakhshan. According to a letter from the French court, the notices sent to Rakhshan's relatives were returned with the notice "Does not live at the address indicated," and a law consultant of the French bank informed the court that Dupont and Fournier did not work at the bank. At the October 26 hearing, the trial court asked Rakhshan to explain his failure to participate in the French Rogatory Commission or to encourage his witnesses to attend. Rakhshan complained that the French procedure was "lengthy and cumbersome" and he wanted a "face-to-face confrontation" rather than the procedure authorized by the trial court. He claimed that he had arranged for his relatives to be deposed in England without any government involvement and offered to pay for the County's attorney to attend the depositions.

The trial court granted the County's motion for protective order and stated that it would not recognize the Fournier deposition based on Rakhshan's failure to participate in the French procedure. The trial court noted that French authorities had reported that the witnesses and participants of the Rogatory Commission had received death threats and had increased security in response. The court also noted that a declaration from Skagit County Superior Court Judge Susan Cook indicated that she received communications from the Rogatory Commission regarding a fraudulent fax bearing her signature and purporting to cancel the Commission. The court also noted that Rakhshan's proposed depositions in England would not include any governmental authority to verify identities or administer oaths. Finally, the trial court stated:

Your witnesses were subject to French authorities, French oath and possible French prosecution if they perjured themselves in that procedure in France. There is no accountability if they fly to England or to Canada for those depositions. That's specifically why this procedure was put in place. I can't explain, Mr. Rakhshan, why you or your witnesses chose not to participate. I'm not holding you responsible for any death threats. But that did not cancel the procedure in any event. All you had to do was submit your questions in writing.[4]

The trial court has the authority to limit discovery where "the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought."[5] Rakhshan rejected the opportunity to obtain evidence from witnesses in France through the procedure authorized by the trial court and French law and instead sought to establish his own procedure for taking depositions, apparently designed to circumvent the participation of any objective government authority. The trial court properly limited discovery.

As to evidentiary matters, Rakhshan contends that the trial court did not address his challenge to the declaration of Brian Korbs under ER 404(b) and ER 403. He also claims that the trial court erroneously denied as untimely his motion to strike various affidavits and testimony as unsworn, containing hearsay, and lacking personal knowledge or expertise. We disagree.

Failure to make a timely motion to strike waives any deficiency in affidavits submitted in support of a summary judgment motion.[6] Here, the motion to strike came after the court's ruling on the motion for summary judgment.

In any event, at the January 11, 2008 hearing, the trial court stated that to the extent the County's evidence could be considered evidence of other acts subject to ER 404(b), it was properly considered to show motive, opportunity, intent, preparation, plan, and knowledge on Rakhshan's part to perpetrate a fraud on others. The trial court determined on the record that the probative value of the evidence outweighed any prejudicial effect. There was no error.

The trial court granted the County's motion for summary judgment at the January 11 hearing. On March 21, Rakhshan moved to strike the County's evidence raising various other objections. The trial court

properly denied the motion to strike as untimely. Moreover, the alleged deficiencies in the evidence received from the French commission did not require exclusion under CR 28(b).

We note that CR 28(b) provides in pertinent part:

Evidence obtained in response to a letter rogatory or a letter of request need not be excluded merely for the reason that it is not a verbatim transcript or that the testimony was not taken under oath or for any similar departure from the requirements for depositions taken within the United States under these rules. Rakhshan's complaint that the testimony obtained through the French court was unsworn does not establish grounds for exclusion. Although some of the declarations did not include certifications under the penalty of perjury as described in RCW 9A.72.058, the County could have remedied the oversight had Rakhshan objected before the summary judgment hearing.

Finally, even if some declarations identified in the motion to strike were not considered, ample evidence supported the decision to grant summary judgment. Even without the testimony of one car dealer, the owner of the car transport service, an individual who bought a car from Rakhshan, and Secret Service Agent Brian Korbs, the County presented other evidence that Rakhshan did not have any legal property interest in the cars. The evidentiary determinations were proper.

SUMMARY JUDGMENT

Rakhshan contends that the trial court erred in granting Whatcom County's summary judgment motion. We disagree.

We will affirm an order granting summary judgment if there are no genuine issues of material fact and the moving party is entitled to judgment as a matter of law.[7] A material fact is one upon which the outcome of the litigation depends.[8] We consider the facts submitted and all reasonable inferences from those facts in the light most favorable to the nonmoving party.[9] When there is contradictory evidence presented, a summary judgment motion should be denied, provided that the contradictory evidence "is not too incredible to be believed by reasonable minds."[10] Summary judgment is proper when reasonable minds could reach but one conclusion regarding the material facts.[11] We review a summary judgment order de novo,[12]conducting the same inquiry as the trial court.[13]

"Conversion is the unjustified, willful interference with a chattel which deprives a person entitled to the property of possession."[14] To maintain a conversion action, the plaintiff must establish some property interest in the converted property.[15]

In support of its summary judgment motion, the County presented evidence that Rakhshan arranged to purchase the cars from various dealerships over the internet and telephone. Rakhshan admitted that he represented a fake, novelty identification card bearing the name "Andrew Rahshan" to be an authentic British Columbia driver's license in order to purchase the vehicles. He sent the dealers copies of several credit cards bearing the bank designation "BDNI" and an account holder name of "Andrew Rahshan." The County presented the declaration of Joseph Majka of Visa U.S.A. Inc., stating that BDNI is an Indonesian bank that has not been a Visa member since 1998, such that any card bearing the BDNI designation and an expiration date beyond 1998 cannot be legitimate. Majka also stated that the routing number appearing on the cards used by Rakhshan is being used under license by Hong Kong and Shanghai Banking Corporation, France ("HSBC"), and would not appear on a BDNI card.

Bank employees Dominique Sonsino and Blaise Ravetto testified before the Rogatory Commission in France that HSBC did not issue the cards and that the account numbers used by Rakhshan were actually issued to other individuals not related to Rakhshan. The account holders contested the charges used to purchase the cars and HSBC reimbursed them, suffering a loss "on the order of 40,000 Euros." Sonsino testified that Fournier did not work at the bank and that Rakhshan's relatives were not authorized users of any of the accounts at issue. The County also produced English translations of French documents provided to the Rogatory Commission including account statements, account holder letters contesting charges, and police reports.

In response, Rakhshan claimed that his relatives in France authorized him to purchase the cars with their credit cards. He claimed that his witnesses, including his relatives and French bank employee Jean-Pierre Fournier, would testify that the account numbers that he used to buy the cars were issued to his relatives by the French bank and that he was authorized to use the accounts. He contended that Dupont, another purported French Bank employee, could verify Fournier's employment at the bank. None of this is believable, as the trial court observed.

Moreover, Rakhshan offered no evidence to dispute Majka's testimony that any card bearing a BDNI designation and an HSBC routing number "would not be a legitimate device for an authorized credit transaction." And Rakhshan's only claim to a legitimate interest in the cars is entirely dependent on the validity of the BDNI cards, which he admitted he used to purchase the cars. In light of these undisputed facts, even if the trial court had considered Rakhshan's deposition of Fournier and the declarations of Rakhshan's relatives, reasonable minds would find his evidence "too incredible to be believed."[16] Because Rakhshan failed to present any evidence to raise a genuine issue of material fact as to whether he had a legitimate property interest in the cars, the trial court properly granted the County's motion for summary judgment.

Finally, Rakhshan argues that the County seized the cars without legal authority, relying on the common law and constitutional provisions. None of these arguments merit further discussion in light of our determination that the court properly granted summary judgment on the record before us.

ATTORNEY FEES

Rakhshan contends that he filed his complaint and declarations in good faith and that his case has merit, such that the award of fees was improper. We disagree.

We review a trial court's decision to impose sanctions under CR 56(g) and CR 11 for abuse of discretion.[17]The trial court must make specific findings indicating explicitly which filings violated the rules and how such pleadings constitute violations or demonstrate bad faith.[18] Here, the award is fully supported by the record.

Although Rakhshan assigns error to a number of the trial court's factual findings, he either does not support the assignments by argument or argues on the basis of matters that are not believable, as the trial court stated.

After making proper findings, the trial court stated its conclusions.

The trial court concluded that Rakhshan submitted the declarations of his relatives, Fournier and Dupont in bad faith in violation of CR 56(g). The court also determined that Rakhshan's complaint was not based on fact or law and thereby violated CR 11. Moreover, because Rakhshan had no property interest in the vehicles, he filed his complaint and proffered evidence for improper purposes, including to further his fraudulent scheme to steal the vehicles. Finally, Rakhshan's bad faith needlessly increased the County's costs and justifies an attorney fee award.

Rakhshan first contends that his complaint was filed in good faith because the County obtained the cars through an unreasonable seizure. But the circumstances under which the County obtained the cars are completely irrelevant to Rakhshan's claim for conversion. His arguments to the contrary are unpersuasive.

Rakhshan also claims that the fee award violates RCW 36.27.050 by allowing the prosecuting attorney to collect fees for his official services. This argument has no merit. The trial court specifically and properly awarded fees to Whatcom County, not the prosecuting attorney.[19]

Rakhshan's remaining challenges to the trial court's findings and conclusions regarding the fee award concern the admissibility of the evidence presented by the County. We perceive of no abuse of discretion in the trial court's analysis of the admissibility of the evidence or the award of fees.

Whatcom County requests fees on appeal under RAP 18.1, arguing that Rakhshan's appeal is frivolous. We agree.

An appeal is frivolous "if no debatable issues are presented upon which reasonable minds might differ, and it is so devoid of merit that no reasonable possibility of reversal exists."[20]

In this case, Rakhshan persisted in his conversion action against Whatcom County despite the lack of any facts or law to support such a claim. Rakhshan's appeal presents no debatable issues and is frivolous. Whatcom County is entitled to costs and attorney fees on appeal, subject to its timely compliance with RAP 18.1.

We affirm the orders on appeal and impose sanctions, as noted.

AGID and GROSSE, JJ., concur.

FOOTNOTES

1. Report of Proceedings (January 11, 2008) at 10.

2. Balise v. Underwood, , 200, (1963).
3. Doe v. Puget Sound Blood Ctr., , 777, (1991).
4. Report of Proceedings (October 26, 2007) at 18-19.
5. CR 26(b)(1)(B).
6. Meadows v. Grant's Auto Brokers, Inc., , 881, (1967).
7. CR 56(c).
8. Greater Harbor 2000 v. City of Seattle, , 279, (1997).
9. Wilson v. Steinbach, , 437, (1982).
10. Balise, 62 Wn.2d at 200.
11. Tran v. State Farm Fire and Casualty Co., , 223, (1998).
12. Folsom v. Burger King, , 663, (1998).
13. Folsom, 135 Wn.2d at 663 (citations omitted).
14. Meyers Way Development Ltd. Partnership v. University Savings Bank, , 674-75, (1996).
15. Meyers Way, 80 Wn. App. at 675.
16. Balise, 62 Wn.2d at 200.
17. Just Dirt, Inc. v. Knight Excavating, Inc., 138 Wn.App. 409, 415, (2007); Biggs v. Vail, , (1994).
18. Biggs, 124 Wn.2d at 193, 201-02; Recall of Pearsall-Stipek, , 266-67, (1998).
19. State v. Weston, , 146 n.2, (1992) (purpose of RCW 36.27.050 is to prevent outside influences on an attorney working for the State, not to prohibit an award of fees to the State as a party).
20. Chapman v. Perera, , 455-56, , review denied, (1985).

The Sydney Morning Herald

Conman hit three Australian banks in credit card sting

Leonie Wood
Published: September 8, 2011 - 12:01AM

A CANADIAN court has found that three Australian banks and many more international banks were defrauded by a Canadian conman who used multiple fake credit cards in 2008 to buy a fleet of luxury cars and a boat.

Westpac, St George Bank and Bankwest were just three of numerous banks and card issuers from around the world whose employees testified this year against Kamyar Jahanrakhshan of North Vancouver.

In spending almost $C500,000 ($A480,000) of other people's money, Jahanrakhshan used forged credit cards that carried his real name and he supplied various car dealers with his driver's licence.

He was found guilty last month of multiple counts of fraud by the Supreme Court in British Columbia.

Employees from Westpac, St George and Bankwest gave evidence that numbers on some of the fake credit cards correlated with genuine accounts issued to their customers.

Earlier this year, Jahanrakhshan was sentenced to six months' jail for impersonating a police officer and obstructing the course of justice.

In that case, the court heard that while under investigation for credit-card fraud in 2008 and 2009, he conned staff at Bankwest and St George into faxing him details of credit-card accounts after telling them he was a Canadian police officer.

In the latest case, Justice Gregory Bowden was told that the Australian banks suffered losses of tens of thousands of dollars as Jahanrakhshan spent more than $C340,000 on cars in the seven months to June 2008.

The court also heard he used many counterfeit cards to buy three BMWs, two Mercedes Benz cars, a 2007 Cadillac Escalade and a 2008 Lexus RX350, as well as a 2006 Sea Ray Sundancer 300 boat valued at $C127,000.

Jahanrakhshan used eight bogus credit cards to pay for one of the BMWs, six to buy the Cadillac and nine to pay for the boat, sometimes using the fake cards multiple times to draw down thousands of dollars.

He was also found guilty of being in possession of devices used for making fake credit cards.

The court heard that when Jahanrakhshan bought one of the BMWs in June 2008, the car dealership's electronic funds terminal transmitted 13 transactions valued at $63,556 against four credit cards over a period of 2½ hours. In that time, a further 21 transactions valued at $137,174 against 12 credit cards were declined.

Card issuers and banks in England, France, Egypt, United Arab Emirates and Brazil were defrauded in the scam.

Exhibit 2

The Sydney Morning Herald

Canadian conman taps banks

Leonie Wood
Published: September 8, 2011 - 12:07AM

A CANADIAN court has found three Australian banks and many more from elsewhere were defrauded by a Canadian conman who, in 2008, used multiple fake credit cards to buy a fleet of luxury cars and a $C126,950 ($121,600) boat.

Westpac, St George Bank and Bankwest were just three banks and card issuers from around the world that gave evidence this year against Kamyar Jahanrakhshan of North Vancouver.

In spending almost $C500,000 of other people's money, Jahanrakhshan used forged credit cards that carried his real name and supplied the various car dealers with his driver's licence.

He was found guilty last month of multiple counts of fraud by the Supreme Court in British Columbia.

Staff from Westpac, St George and Bankwest gave evidence that numbers used on some of the fake credit cards correlated with genuine accounts issued to their customers.

Jahanrakhshan was sentenced this year to six months' jail for impersonating a police officer and obstructing the course of justice. The court heard that while Jahanrakhshan was under investigation for credit-card fraud in 2008 and 2009, he conned staff at Bankwest and St George into faxing him details of credit card accounts after telling them he was a Canadian police officer.

In the latest case, Justice Gregory Bowden heard that the Australian banks suffered losses of tens of thousands of dollars as Jahanrakhshan spent more than $C340,000 on cars in the seven months to June 2008.

The court heard Jahanrakhshan used counterfeit cards to buy three BMWs, two Mercedes Benz cars, a 2007 Cadillac Escalade and a 2008 Lexus RX350, as well as a 2006 Sea Ray Sundancer 300 boat.

Jahanrakhshan used eight bogus credit cards to pay for one of the BMWs, six to buy the Cadillac and nine to pay for the boat, sometimes using the fake cards multiple times to draw down thousands of dollars.

He was also found guilty of being in possession of devices used for making fake credit cards.

The court heard that when Jahanrakhshan bought one of the BMWs in June 2008, the car dealership's electronic funds terminal transmitted 13 transactions valued at $63,556 against four credit cards over a period of 2½ hours. A further 21 transactions valued at $137,174 against 12 credit cards were declined in that time.

Card issuers and banks in England, France, Egypt, United Arab Emirates and Brazil were also defrauded.

Exhibit 3

Canadian conman taps banks

Leonie Wood
7 Sep 2011, 8:12 p.m.

A CANADIAN court has found three Australian banks and many more from elsewhere were defrauded by a Canadian conman who, in 2008, used multiple fake credit cards to buy a fleet of luxury cars and a $C126,950 ($121,600) boat.

Westpac, St George Bank and Bankwest were just three banks and card issuers from around the world that gave evidence this year against Kamyar "Andy" Jahanrakhshan of North Vancouver.

In spending almost $C500,000 of other people's money, Jahanrakhshan used forged credit cards that carried his real name and supplied the various car dealers with his driver's licence.

He was found guilty last month of multiple counts of fraud by the Supreme Court in British Columbia.

Exhibit 4

Staff from Westpac, St George and Bankwest gave evidence that numbers used on some of the fake credit cards correlated with genuine accounts issued to their customers.

Jahanrakhshan was sentenced this year to six months' jail for impersonating a police officer and obstructing the course of justice. The court heard that while Jahanrakhshan was under investigation for credit-card fraud in 2008 and 2009, he conned staff at Bankwest and St George into faxing him details of credit card accounts after telling them he was a Canadian police officer.

In the latest case, Justice Gregory Bowden heard that the Australian banks suffered losses of tens of thousands of dollars as Jahanrakhshan spent more than $C340,000 on cars in the seven months to June 2008.

The court heard Jahanrakhshan used counterfeit cards to buy three BMWs, two Mercedes Benz cars, a 2007 Cadillac Escalade and a 2008 Lexus RX350, as well as a 2006 Sea Ray Sundancer 300 boat.

Jahanrakhshan used eight bogus credit cards to pay for one of the BMWs, six to buy the Cadillac and nine to pay for the boat, sometimes using the fake cards multiple times to draw down thousands of dollars.

He was also found guilty of being in possession of devices used for making fake credit cards.

The court heard that when Jahanrakhshan bought one of the BMWs in June 2008, the car dealership's electronic funds terminal transmitted 13 transactions valued at $63,556 against four credit cards over a period of 2½ hours. A further 21 transactions valued at $137,174 against 12 credit cards were declined in that time.

Card issuers and banks in England, France, Egypt, United Arab Emirates and Brazil were also defrauded.

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

UNITED STATES OF AMERICA

v.

KAMYAR JAHANRAKHSHAN, also known as KAMYAR JAHAN RAKHSHAN; ANDY or ANDREW RAKHSHAN; ANDY or ANDREW KAMYAR (or KAMIAR or KAMIER) RAKHSHAN

WARRANT FOR ARREST

NO. 3:16mj636-BK

YOU ARE HEREBY COMMANDED to arrest KAMYAR JAHANRAKHSHAN, also known as KAMYAR JAHAN RAKHSHAN; ANDY or ANDREW RAKHSHAN; ANDY or ANDREW KAMYAR (or KAMIAR or KAMIER) RAKHSHAN and bring him forthwith to the nearest magistrate to answer a

☐	Indictment	☐	Information	☒	Complaint	☐	Order of Court	☐	Violation Notice	☐	Probation Violation Petition

charging him with (brief description of offense) knowingly causing the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally causing damage without authorization to a protected computer; in that the defendant knowingly caused a denial of service attack on the website Leagle.com, and by said transmission caused a loss aggregating at least $5,000 or more during a one-year period.

In violation of 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(c)(4)(A)(i)(I) and (B).

RENÉE HARRIS TOLIVER
Name of Issuing Officer

Signature of Issuing Officer

Bail fixed at $ _____ by

UNITED STATES MAGISTRATE JUDGE
Title of Issuing Officer

JULY 29, 2016, DALLAS, TEXAS

_____
Name of Judicial Office

RETURN

This Warrant was received and executed with the arrest of the above named defendant at

DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE OF ARREST		

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu