

DOJ and FBI Whistleblower Cover-up Hid From President Trump and Staff His Entire Term

I am one of five federal whistleblowers and a disabled US Air Force veteran in Kapolei, Hawaii near Honolulu who has been under illegal movement surveillance, cell phone wiretapping, and computer destruction by the US Army or its agents for nearly six long years. The whistleblowing involved the documented abuse of a US Army soldier who after being discharged died under mysterious circumstances law enforcement will not investigate. Because of the whistleblowing, my family and I have suffered terrible retribution and retaliation since June 2016. Only by the grace and help of Christ Jesus after so much resistance and blocks am I able to post this notice now.

Repeatedly and incessantly, I've asked the FBI and the Honolulu Police Department (HPD) to intervene and waited and waited but neither agency will investigate forensic, visual, and other irrefutable evidence I've provided. The FBI will not answer nearly 25 FBI IC3 cybercrime complaints I've filed. HPD rushed to close out 30+ cybercrime cases on file from 2016-2022 when asked to formally refer an international cyber crime case to the FBI. I am threatened with jail if I file another case dated before October 18, 2022.

I've asked Hawaii Democratic senators to help me. Neither one will offer help. Other whistleblowers have asked their respective Democratic senators to intervene. None acted to any benefit. This is all done to keep the abuse and ultimate demise of the soldier and persecution of my family and I and the other whistle blowers silent and hidden.

The Army cyber criminals disabled or destroyed nine of my computers between March 13 to May 14, 2022. I filed a police report under case #21-151824 assigned to HPD Detective Pait for each of five desktop and laptop computers infected. Although I presented evidence proving my computers had been compromised through the installation of an unencrypted connection that allowed operating system software to be replaced, HPD states they cannot find any financial loss. Earlier after a previous compromise, the Deputy Chief of Police would not respond to my appeals for help sent when I had no secure online capability during the worst of COVIT-19. At a meeting held on 12/17/21 at the Honolulu Police Department main station, HPD officer Lt Andrew Maddock expressed his opinion that I am paranoid, psychotic, and imagining every one of the events I've conveyed with a request for law enforcement investigations. After filing five new crime statements in seven months with no action followed by a complaint against Lt Maddock for negligence I was assigned a new case officer, my eighth. Immediately, cyber crime evaluations were based on admitted opinions and guesses I documented. More delay tactics applied ending in HPD closing all my cases to keep them hidden.

Cover-up by DOJ, FBI, US Army:

On September 3 2020 I sent a letter to Department of Justice Attorney General Barr explaining my circumstances and the reason for the whistleblowing along with a request to help me. Four months later on the day President Trump left office I received a non-sense, evasive reply not from the DOJ, not from the FBI, but from the Army, the same agency that has, and continues to persecute me and my family to this day.

Consider the response to my letter sent to AG Barr. Compare the content in the reply against the facts I expose surrounding the soldier's abuse and ultimate demise. A logical comparison absolutely erases the possibility what I claim is not true.

The non-response was very purposely hidden from President Trump's staff during his last months in office and not provided to me until January 21, 2021. Again, I mailed my letter to AG Barr on September 3, 2020. The reason for the whistleblowing was hidden during his entire term.

Thus goes the cover up. It is the reason for the criminal retribution against me for the past 6 1/2 years.

In its totality, the length and expanse of the victimization has been truly .

Please go to these evidence sites to see proof of my claims: <https://bit.ly/3sDztgi>

<https://bit.ly/808cybercrime>
<https://bit.ly/2Wfree76>
<https://bit.ly/3D2m8qk>

<https://bit.ly/3uvzOD1>
<https://bit.ly/3MudU9n>

<https://bit.ly/3vkCsvs> (Update)

Dr. Cassandra Harrell, sister of the dead soldier

No answer to presidential query
cassandraharrell@comcast.net

(601) 782-2092, (678) 891-9558

Mrs. Sharon Rondeau, online newspaper editor Postemail.com

editor@postemail.com info@postemail.com

(203) 987-7948 (860) 556-9392

Pastor Gary Mason, the soldier's family pastor

(202) 531-8148

gmock70@hotmail.com

gary.mock@ameritrade.com

gmock@msn.com

shanaaz.mason@yahoo.com

**Honolulu Police Dept Detective
Thomas linuma (808) 723-3592
tiimuma@honolulu.gov closed
all cases to avoid referral to FBI.**

**Editor Rondeau has written dozens of stories about the
coverup: <https://www.thepostemail.com>**

**Det linuma failed to interview Dr. Harrell because doing so would force an
interstate referral to the FBI. The FBI doesn't want to investigate my case
and expose the cover up. Dr. Harrell sent several emails, made phone calls,
and left voice messages for Det linuma who did not reply until the time was
right as he stated.**

I continue to receive relentless and extremely sophisticated cyber attacks trying to keep me silent. The cyber criminals disabled my virtual protection networks (VPN's) to ensure I couldn't disappear online. Cyber criminals have intercepted and stolen evidence documentation I've sent via UPS to the Epoch Times newspaper.

I presented collaborators waiting to validate my claim my cell phone is illegally wiretapped the same as theirs. One of the collaborators, Dr. Harrell, the sister of the dead soldier, is waiting to be interviewed for the opportunity to tell law enforcement the identity of the cyber criminals and their attack location. I asked HPD to call Dr. Harrell. No one will call her.

The wiretapped cell phones are the most damaging attack of all. The Army cyber criminals cloned my phones and snoop in on planning discussions between network engineers, computer technicians, and I. Selected cell phone discussions are scrambled or blocked. My text messages are intercepted and read. Text messages I write are remotely written to and altered. My standard email in my phone and computers is subjected to Man-In-The-Middle attacks and read.

I presented collaborators waiting to validate my claim my cell phone is illegally wiretapped the same as theirs. One of the collaborators, Dr. Harrell, the sister of the deceased soldier, is waiting to be interviewed for the opportunity to tell law enforcement the identity of the cyber criminals and their attack location. Again and again I've asked HPD to call Dr. Harrell. No one will.

As the FBI and HPD refuse to investigate any leads or unarguable proof I offer, I continue to present court-ready forensic evidence proving my phones are illegally wiretapped for surveillance backed by Verizon phone logs. I've given carrier phone records disclosing, the street, city, state, and phone number of a call that installed remote control malware to control my iPhone's microphone and camera for surveillance.

Since March 3, 2021 the Army cyber criminals have remotely attacked and disabled eight of my computers. Scans of the operating system unquestionably revealed "backdoor" uploads of native, but expired Windows software banned since 2017 as security risks. Army cyber criminals replaced original onboard registry files that passed through a malicious unsecured web link.

Please speak with the other whistleblowers who like me, have been robbed of their right to privacy, ability to earn a living, and other rights under the Constitution.

Remember, the existence of a cover up is evidence a crime occurred. Even if the cover up does not show the details or the nature of the crime itself, a cover up shows that there is something shady going on, or those persons involved or group is trying hard to hide something. In this case, there is a five year history of cyber crime incidents against me and

Contact: Ricardo A. Finney

92-1206 Hookeha Place

Kapolei, HI 96707

(808) 255-9701

nikon@precisionphotography.live

finney808@proton.me

ricardof@mailfence.com

the other whistleblowers, preceded by three years of criminal activity surrounding the abuse of the now-dead soldier.

I very urgently need this help:

- An investigative reporter to expose the facts
- Honest law enforcement intervention
- A path to recover from the Nation-State level cyber attacks
- Prayer, prayer, and more prayer.

Please investigate and expose this. Please contact me and the others as soon as possible. My attorney and I await your phone call or email (encrypted preferred) sent to atp@atphillips.com and nikon@precisionphotography.live

Very Respectfully,

Mr. Ricardo A. Finney
US Air Force (Retired)
92-1206 Hookeha Place
Kapolei, HI 96707
(808) 255-9701
thunder707@protonmail.com
ricardof@mailfence.com
depth99@protonmail.com



Six

For nearly ~~five~~ years I and four other federal whistleblowers against the US Army have been under illegal surveillance by cybercriminals and illegal wiretappers. Conspirators kept this evidence letter I wrote to Attorney General Barr at the DOJ hidden from President Trump's circle from 9/9/20 thru the Inauguration. Sent last fall, they sat on my letter for four months and eighteen days to prevent its viewing and subsequent repercussions. Preceding this, politicians would not help.

The FBI, the action addressee, (routed through the DOJ) did not reply. Instead, on 1/21/21, US Army conspirators emailed the attached non-response dated 1/19/21 to me. I submit their letter, dated on the last day of the administration, and their email, delivered the day after the change, was purposely hidden.

<https://bit.ly/3vkCsvs> (Update)

This is why...
<https://bit.ly/380QUg8>

Mr. Ricardo A. Finney
92-1206 Hookeha Place
Kapolei, HI 96707-1544
(808) 255-9071 (808) 384-0294
Encrypted email: raineer44@lionofjudah808.live
"The Lion Of Judah remains on His Throne"

Mrs. Sharon Rondeau
Editor, The Post & Email Online Newspaper
<https://www.thepostemail.com>
editor@thepostemail.com
203 987-7946

Ms. Cassandra Harrell
Deceased US Army soldier's sister
(601) 782-2092 mscyharrell@gmail.com
(678) 891-9558

Remember, the existence of a cover-up is evidence a crime occurred. Even if the cover-up does not show the details or the nature of the crime itself, a cover-up shows that there is something shady going on that a person or a group is trying hard to hide. In this case, there is a four-year history of cybercrime incidents against me and the other whistleblowers, preceded by three years of criminal activity surrounding the abuse of the soldier.

I requested investigative action by the FBI. Instead, I received a letter not from the FBI, but from my suspected attackers, the US Army. I continue to ask for law enforcement intervention from the FBI who refuses to respond to nearly 25 IC3 complaints filed from 2016 through 2022.

September 3, 2020

To: Attorney General William Barr
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

From: Mr. Ricardo A. Finney
92-1206 Hookeha Place
Kapolei, HI 96707-1566
lionofjudah808@protonmail.com
808 255-9701 (*Wiretapped*)

In my letter dated September 3, 2020 addressed to Attorney General Barr at the Department of Justice, I refer to the Federal Bureau of Investigation eight times requesting intervention.

On January 21, 2021, 4 months and 18 days later, I received a reply from the Department of the Army, the same agency in which I registered my complaint against asking for FBI assistance.

Subject: Request for Intervention/Civil Rights Violations

Many of my constitutional rights have been violated through repeated very sophisticated cyber crimes and illegal surveillance conducted by the US Army or its agents. I respectfully request that you intervene and task the FBI to protect me. In July 2016 I was a federal whistleblower against the US Army. In retaliation, for the past 4+ years the military or their civilian hires have, and continue to conduct around-the-clock, highly sophisticated cyber attacks against my family and I that have infected or disabled nearly every computer, tablet, digital camera, and cellphone we have. They have placed us under constant illegal video, audio, cellphone, and movement surveillance. Their objective is to keep the reasons for the whistleblowing hidden and silent. Please read this information and the links attached to learn why:

<https://www.thepostemail.com/2020/03/10former-us-army-soldier-found-deceased/>

Since August 2016 I have repeatedly asked the FBI to help me to no avail. I'm sent five submissions to their IC3 website, made 9 personal visits to the Kapolei, Hawaii Field office to speak with agents, and submitted five written letters pleading for protection. Within all, I've asked for intervention to stop the illegal wiretapping and other criminal acts. The FBI has stayed silent and will not intervene.

Nothing has been done to stop the cyber attacks, illegal wiretapping, and illegal surveillance since this was written in 2018:

<https://www.thepostemail.com/2018/01/20/report-cyberstalked-hawaii-resident-receives-no-assistance-state-government/>

Because of the violent nature of the crimes against the soldier, I've repeatedly expressed concern for the safety of my family and I, again to no avail.

At great personal expense I've provided the FBI with forensic evidence proving my computer devices were compromised and the level of sophistication involved. I've provided the physical address and phone number of a person who illegally accessed my cellphone for wiretapping. I've given contact information for a vendor who has the location of computers used to steal my security software licenses. I've provided proof of wiretapping received from my cellphone carrier and much, much more solid evidence and

leads. I've stored enough additional electronic evidence to trace the cyber criminals to their doorstep(s).

My digital evidence files and other physical items will provide a direct trail to the criminals, however the FBI will not put in the work. The daily retaliation continues. I sent this correspondence via surface mail instead of using your "Contact Us Form" because the cyber criminals infected my business network and outbound email again. However, against great resistance I was able to post online a small portion of the forensic, physical, and other evidence to support my claims:

<https://bit.ly/808vbercrime>

nacked

~~<https://bit.ly/3gLUc8V>~~

<https://bit.ly/380øug8>

<https://bit.ly/2RLBbXT>

<https://bit.ly/2P6dquO>

The constant cyber attacks completely destroyed my small business, caused our forced retirement from the work force, decimated our bank and retirement savings, drastically increased our daily stress, brought about a decline in our physical health, and caused numerous other severe impositions on our constitutional right to privacy. On August 21, 2020 I contacted Senator Brian Schatz (D) Hawaii for help. I have not received a reply.

After my most recent appeal for intervention last month failed, I noted it is especially cruel I cannot get the agency's help even in the midst of the COVIT-19 pandemic with Internet access so essential to daily living.

The actions of the cyber criminals continue to violate my civil liberties to include the right to privacy, freedom of expression, and unreasonable search. The United States Constitution protects these rights, including the right for my wife and I to operate our small businesses without forced illegal shutdowns. In an article published by Fox News on 9/1/20, a spokesperson from the FBI's Chicago field office told Fox News this:

"The FBI's mission has always been to protect the American people and uphold the Constitution of the United States"

<https://www.foxnews.com/us/chicago-police-confirms-gang-threat>

As a disabled military veteran who served this nation with honor and distinction for nearly 30 years, I believe I've more than earned the right to have the FBI to protect me from the cyber criminals who continue to violate my civil rights. I ask that you intervene and task the FBI to act on my behalf without further delay. Please contact me as soon as possible with your determination. Feel free to call my wiretapped cellphone number, 808 255-9701. I want the criminals to know what has happened to me finally has high-level attention and is no longer hidden. Thank you.

Best Regards,

Ricardo Finney

Ricardo Finney
Kapolei, Hawaii

Categorize Snooze Undo

Response to Presidential Correspondence

S/MIME isn't supported in this view. To view this message in a new window, [click here](#)

U USARMY Pentagon HQDA OTIG Mailbox IGMET SAIG AC Whistleblower Rep <usarmy.pentagon.hqda-otig.mbx.ignet-saig-ac-whistleblower-rep@mail.mil>

Thu 1/21/2021 2:21 AM
To: Raineer 44

*My submission to AG Barr sent Sep 3, 2020
Email from US Army sent Jan 21, 2021
Reply dated Jan 19, 2021*

 Final Response TMT HQDA-2...
2 MB

Mr Finney

Please find our attached response on behalf of the POTUS, regarding the correspondence you sent to him regarding your whistleblower protections.

Respectfully,

US Army Inspector General Agency
Assistance Division (SAIG-AC)
Whistleblower Reprisal / Improper MHE
1700 Army Pentagon, Rm 3038
Washington, DC 20310-1700

INSPECTOR GENERAL CONTROLLED UNCLASSIFIED INFORMATION: The information contained in this email and any accompanying attachments may contain Inspector General Controlled Unclassified Information, which is protected from mandatory disclosure under 5 USC 552. Matters within IG records are often pre-decisional in nature and do not represent final approved DA policy. Dissemination is prohibited except as authorized under AR 20-1. Do not release outside of DA channels without prior authorization from The Inspector General. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action in reliance on this information is prohibited. If you received this email in error, please notify us immediately by return email or by calling 703-614-2770.
CUI

[Reply](#) | [Forward](#)

The Army's email announcing their attached reply arrived nearly four months after my query was received and is dated one day AFTER President Trump left office. Their reply to my query written to AG Barr requesting FBI intervention is dated one day BEFORE President Trump left office.



DEPARTMENT OF THE ARMY
U.S. ARMY INSPECTOR GENERAL AGENCY
1700 ARMY PENTAGON
WASHINGTON, DC 20310-1700

January 19, 2021

Assistance Division

Mr. Ricardo Finney
92-1206 Hookeha Place
Kapolei, HI 96707-1566

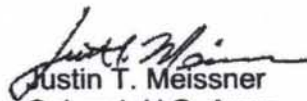
Dear Mr Finney:

Thank you for your recent correspondence to President Donald J. Trump concerning your whistleblower reprisal protections in regards to exposing medical treatment matters within the United States Army.

The United States Army Inspector General Agency has reviewed your documentation and determined that you are not protected under Title 10 United States Code, Section 1034, "Military Whistleblower Protection Act," Protected communications; prohibition of retaliatory personnel actions. In addition, your concerns that you have raised pertain to cyberattacks and surveillance, which we considered not appropriate for the Inspector General to address. The proper avenue of recourse for these matters lies within law enforcement and federal agencies, specifically, the Federal Bureau of Investigation. We recommend you contact a local field office in your area or visit the Bureau's website to submit your claim.

Our office will take no further action in this matter and consider it closed. Should you have any further questions, you can reach my action officer, Mr. Alex Bishop, 703-545-2122 or email alex.w.bishop.civ@mail.mil.

Sincerely,


Justin T. Meissner
Colonel, U.S. Army
Chief, Assistance Division

My request for intervention was sent to Attorney General Barr at the Department of Justice, not to the outgoing President Trump who left office the day before the email was sent to me. I asked for FBI assistance, not from the US Army, the agency against which I made my whistleblower claim.

The "recent" response came 4 months and 18 days after my letter to AG Barr.

This reply sends me back to the same federal agency I repeatedly have requested assistance from.

Army leadership knew the history about the abused soldier and in turn the abuse against me when they sent this non-answer. At the time this correspondence was written, I had sent six cyber crime complaints to the FBI. Since then I have sent 16 more with no reply.

When this non-answer was sent, Army leadership at the highest level and beyond knew about the abused soldier, and in turn my persecution. This was driven by the soldier's sister successfully filing for a presidential query. She never received a reply. Either illegally the query wasn't referred, or if it was referred it was ignored.

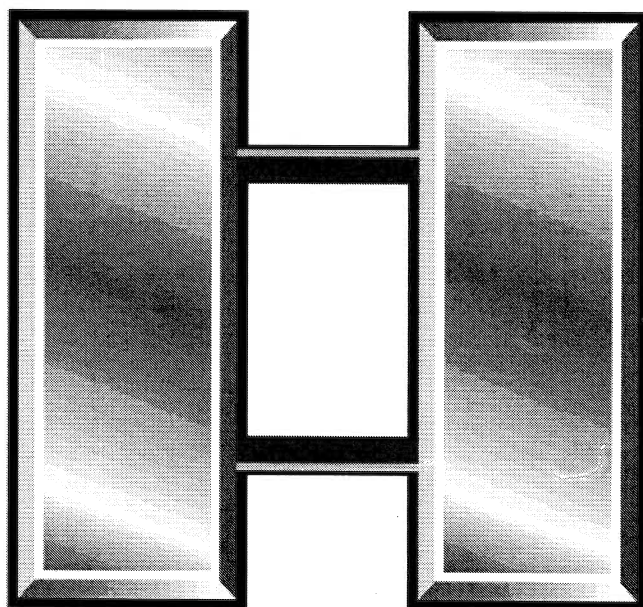
Former U.S. Army Soldier Found Deceased

On Tuesday, March 10, 2020 · No Comment

If you're new here, you may want to subscribe to my free Email alerts. Thanks for visiting!

A VICTIM OF MILITARY SEXUAL ASSAULT

by Sharon Rondeau



U.S. Army Captain's insignia

(Mar. 10, 2020) — On Tuesday morning, The Post & Email learned from a family member that a former U.S. Army captain whose story we covered beginning in June 2016 is deceased.

As we reported, in 2014 the soldier was sexually assaulted while on active duty and suffered a traumatic brain injury at the hands of his attackers. He also was financially victimized through fraudulent signature loans, the perpetrators of which have never been identified.

The soldier's power of attorney at the time reported difficulties in obtaining his medical records through Walter Reed National Military Medical Center as well as treatment for the soldier's trauma. However, she believed he was over-medicated and that a

“cover-up” of the crimes committed against the soldier was ongoing. “Millions of soldiers and Americans suffer from mental illness,” the former POA told us on October 15, 2016. “Looking at the stats, how many soldiers are really suffering from mental illness versus how many are just given a ‘mental illness’ diagnosis to disprove their credibility?”

Last April, we reported that a fellow soldier accepted a plea agreement with the government in connection with multiple electronic thefts of the soldier’s savings from his Navy Federal Credit Union (NFCU) account. The monies were eventually restored, his former POA said.

The soldier was discharged from the Army in early 2017 and experienced several setbacks in his new civilian life, the former POA told us. Police are investigating his death, she said on Tuesday, and more details will be provided when they are available.

◆ mental illness, U.S. Army Soldier, Walter Reed National Military Medical Center

Former U.S. Army Soldier Found Deceased added on Tuesday, March 10, 2020



Sharon Rondeau

Sharon Rondeau has operated The Post & Email since April 2010, focusing on the Obama birth certificate investigation and other government corruption news. She has reported prolifically on constitutional violations within Tennessee’s prison and judicial

systems.

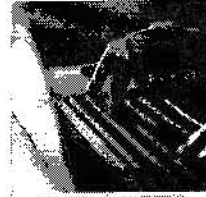
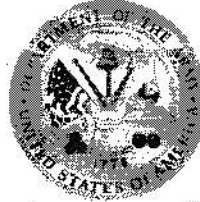


Loading...

We Recommend...

2017 JANUARY						
SUN	MON	TUE	WED	THUR	FRID	SAT
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

ALTER REE
ARMY MEDICAL CEN



U.S. Army Soldier
Not Yet Relocated
from Walter Reed

Will a Real
"Investigation"
Take Place at
Walter Reed...

Perpetrator of
Bank Heist
Against Army
Soldier Sentenced

After Almost Two
Years, Electronic
Military Heist
Remains Unsolved



Report: Former
Soldier's Bank-
Account Breaches
Under
Investigation



Alleged Attempted
Murder,
Brutalizing and
Cover-Up of
Crimes Against
U.S. Army Soldier
Go Unpunished
for More Than
Three Years

The Post & Email

Thursday, August 4, 2016

ABOUT US/COPYRIGHT POLICY PLACE AN AD DONATE CONTACT US

Articles By Month Search in site...

Home » Search results for walter reed

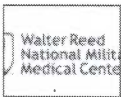
Were the Khans "Attacked," or Did They Launch an Attack?



Tweet MEMBERS OF CONGRESS, MEDIA MAKE STATEMENTS...BUT DID THEY ASK THE RIGHT QUESTIONS? by Sharon Rondeau (Aug. 1, 2016) — On Monday morning, chairman of the House Armed Services Committee...

Monday, August 1, 2016 · 5 Comments · Read More

Why Won't Walter Reed Medical Center Release Soldier's Medical Records?



Tweet "SMOKE AND MIRRORS" by Sharon Rondeau (Jul. 27, 2016) — More than 70 days ago, the first power of attorney (POA) for a U.S. Army soldier injured in 2013...

Wednesday, July 27, 2016 · No Comment · Read More

Does a Tennessee District Attorney Have the Right to Influence the Board of Parole?



Tweet "THEY DON'T CARE AND THEY WON'T CORRECT IT" by Sharon Rondeau (Jul. 22, 2016) — Over the past 30 days, The Post & Email received two letters from TDOC...

Friday, July 22, 2016 · No Comment · Read More

Alleged Attempted Murder, Brutalizing and Cover-Up of Crimes Against U.S. Army Soldier Go Unpunished for More Than Three Years



Tweet "RAPE IN THE MILITARY MUST STOP" by Sharon Rondeau (Jul. 6, 2016) — "People speak sometimes about the 'bestial' cruelty of man, but that is terribly unjust and offensive..."

Wednesday, July 6, 2016 · No Comment · Read More

Recent Comments

- Ed Sunderland on Congressman Tells Constitutional Educator: "Congress Can Vote Anything In That They Want To"
- Gerald W. Buess on With His Fake Birth Certificate and Selective Service Form, Obama Claims Trump "Unfit" to be President
- ELMO on Congressman Tells Constitutional Educator: "Congress Can Vote Anything In That They Want To"
- JONATHAN DAVID MOOERS on With His Fake Birth Certificate and Selective Service Form, Obama Claims Trump "Unfit" to be President
- James Carter on With His Fake Birth Certificate and Selective Service Form, Obama Claims Trump "Unfit" to be President

Search in Archive

Select a date

Select month

Select a category

Whistleblower #4: Ms. Sharon Rondeau, Canterbury, Connecticut

(203) 987-7948 editor@postemail.com info@postemail.com

Please contact the editor of the Post And Email Online, www.postemail.com, Mrs. Sharon Rondeau. Ms. Rondeau has covered the story about the soldier from 2016 to March 2020, his circumstances, and those of Pastor Mason. She covered my story up to 2018. Law enforcement has done nothing to investigate the crimes against me since she wrote this article in 2018 explaining my plight:

<https://www.thepostemail.com/2018/01/20/report-cyberstalked-hawaii-resident-receives-no-assistance-state-government>

<https://productforums.google.com/forum#!msg/play/LxrVBSgWJgE/LfQtor2yAQAJ>

<https://www.thepostemail.com/2018/01/20/report-cyberstalked-hawaii-resident-receives-no-assistance-state-government/>

Report: Cyberstalked Hawaii Resident Receives no Assistance from State Government

On Saturday, January 20, 2018 No Comment **Saturday, January 20, 2018**

If you're new here, you may want to subscribe to my free Email alerts. Thanks for visiting!

BUT WHY?

by Sharon Rondeau



(Jan. 20, 2018) – A disabled Air Force veteran and Hawaii citizen who has reported cyberstalking, hacking, disabling of his electronic

equipment and personal surveillance for nearly 18 months continues to be refused assistance by the Honolulu Police Department and the City & County of Honolulu Department of the Prosecuting Attorney, according to the victim.

The Post & Email has spoken with Detective Choi of the HPD and with Chris Duque, cybercrime investigator for the Prosecuting Attorney's office, and verified that they are not currently investigating the victim's complaints despite the fact that they appear to fall under Hawaii's updated "Cyber Harassment & Stalking" law.

Army's
motive

The victim was instrumental in assisting a family whose soldier relative had reported a 2013 sexual assault, after which he suffered a traumatic brain injury and was hospitalized at Walter Reed National Medical Military Hospital (WRNMMH) for approximately three years, interspersed with stays at facilities providing therapy for memory loss and other neurological impairments.

Mutual
cyber
attacks

In July 2016, the soldier's POA reported that her Yahoo! email account was hacked, along with her children's bank accounts, her work laptop computer, and a brand-new telephone. Shortly thereafter, the Hawaii victim, who had been in regular communication with the POA, experienced the successive disabling of multiple pieces of electronic equipment, interference with costly wi-fi firewalls, and what he described as surveillance of his daily movements and telephones.

Both the Hawaii victim and POA believe that the perpetrators are connected to the U.S. military based on the sophistication of the attacks. ←

The Hawaii victim has visited the FBI in Kapolei on five occasions and submitted more than 20 police reports to the HPD, with new new reports filed over the last week. Many of his reports include analyses from Apple computer professionals.

FBI stopped
visits. HPD
would not
investigate
30+ reports
thru 2022

The Post & Email has submitted a FOIA request to the FBI for any documentation it might possess on the victim's complaints but failed to receive even the standard FOIA acknowledgement letter, much less any documentation.

In October, Choi and Duque told this writer that they were not actively pursuing the perpetrators of the alleged crimes. Choi stated that although the victim's complaints were assigned to him, his expertise is in the field of "forgery." He said that while a new HPD cybercrimes unit is under development, he referred the victim's case to the local FBI by telephone. ←

Duque, for his part, said that if sufficient evidence pointing to a perpetrator or perpetrators of a crime is not received "within 30 days" of the reporting of a crime, his office does not prioritize the case. At the time we spoke with him on October 20, 2017, Duque told us that it appeared to him that the hackers could be using the resources of the federal government to commit their crimes against the victim.

He also suggested a "rogue actor" or someone from the "dark web" as a possible perpetrator. ↑

Duque's determination

Increased
to \$2.5m in
losses plus
40+ hard
drives and
devices
hacked
through
2022

The victim recently employed an attorney to assist him in gaining access to government services. However, following a 17-minute telephone call with Duque last week, the victim reported that Duque's position remains that there are insufficient "resources" within the prosecuting attorney's office to commit to identifying the perpetrators of the reported cyber-crimes.

"He said he needs 'hard evidence,'" the victim told us on Friday, "but if you look at those links [at the prosecuting attorney's website], this should have been solved a long time ago."

The victim has reported business losses surpassing \$140,000 and the disabling of more than 18 computers and telephones in the aggregate over the last year and a half.

There is currently an FBI investigation into corruption at the Honolulu Police Department, whose now-retired police chief, Louis Kealoha, and his wife, deputy prosecutor Katherine Kealoha, are targets, according to Hawaii News Now.

Coincidentally, a federal grand jury probe has been ongoing of the couple since shortly before the Hawaii resident began reporting the cybercrimes. In June 2016, the Kealohas filed a lawsuit claiming that corruption at the Hawaii Ethics Commission motivated that body's probes into their official actions.

Earlier this month, the commission announced the resignation of its executive director, Chuck Tutto.

A related case involving Katherine Kealoha centered on a reported "stolen mailbox," a retired police officer, and an FBI civil rights investigation.

"I've asked for something as simple as the police records, but the detective won't move," the Hawaii victim told The Post & Email. "Unless he closes the case, I can't get the records. But he won't act or return phone calls. It sits there and looks good on paper, but nothing gets done."

Letter from soldier's sister after his death

4/12/2021

Greetings Ricardo,

I hope all is well with you and your family. I am writing this letter to update you as well as to let you know that I pray for you and Clara and I have not given up on justice. It has been very difficult for my family accepting the loss of Casey. I know that he is no longer suffering from the issues of life, mainly the injustices inflicted upon him by the military. We just laid his remains to rest in Arlington on last month. One whole year later. This provided some relief for my mother but the challenges of grief has overwhelmed her. She is strong in the Lord but she won't let go of the guilt or feeling as if she could have done more to help him. I will never be able to repay you for your sacrifice. Without your knowledge and support he would have been locked away until his last days. I know in helping us, the military demons have attacked you and your family beyond anything any of us could have anticipated. I pray that God has broken this demon attack and that you are blessed

in healthy finances; family.

I continue to research and look for people to connect with regarding the cyber attacks and stalking. It is very challenging as people tend to think that I am telling tall tales. I lay low and don't use much technology. Periodically, random cars sit in front of my home. A couple of times I've had to brandish a firearm to send a message before the stalkers retreated. It has been quiet lately but I never know when they will show up. I still have to go to office depot to print out documents and stuff due to wifi.

On another note, I really believe there was foul play in Casey's situation. The authorities are ruling it an accident but I just don't believe them. When I ask questions such as "Where is the camera footage?" There are cameras in the area but the investigator dodges the inquiry. Or other questions such as "Was the taxi/cab driver questioned regarding his role in dropping Casey in a public park by a river front?" "Were there any arrangements to pick Casey up from the park?" "How did he pay →

for the taxi?" "Why was all of Casey's personal effects still on him when his body was discovered (i.e. Gold necklace, wallet w/ credit/debit cards etc.?" "Does the park camera show if he meet anyone when he was dropped off at the park?" There is no interest in helping us to understand what happened. They simply ruled "accidental - case closed!" I know in my heart this ruling was to shut ^{us} up from opening a can of worms regarding the military. Consider this, the military prosecutor's office (handling Hill's case) is only 20 minutes from Casey's old apartment. Apparently, military personnel visited him at his apartment prior to Hill's trial. It's just all weird but I know how they operate. Anyway, I just wanted you to know that I have not turned my back on you and your family. I'm just staying under the radar until we can bring this evil to light. Please continue to pray and take care of yourself. They want to silence us. God is our shelter and he will vindicate us. I will talk to you soon.

Take Care
Cassandra

In this message from Ms. Harrell, she validates her computers were hacked and her phones wiretapped after her involvement with the Army. She also validates her connection to me. This message was sent to Detective Maddock at HPD. She invited him to call. When no call was made, I contacted Detective Maddock and requested he call Ms. Harrell to verify her circumstances and her connection to me. No call was made. Please contact Ms. Harrell to verify this.

December 6, 2017 2016

To: HDP | Detective

Re: Cyber Attacks

Greetings Detective,

My name is Cassandra Harrell, and I reside in the State of Georgia. Over the past five years, I've consistently and without cease advocated for my brother. My brother, an active duty status Captain in the United States Army, was sexually assaulted, robbed of \$13,000 from Navy Federal and beaten because he was a whistleblower while stationed in South Korea.

Over seven months ago, advocates (one being Mr. Ricardo Finney) and myself, unveiled the heinous crimes committed against Capt. Harrell. The crimes and unscrupulous practices of several active duty personnel were reported in a Congressional to U.S. Senator Kirstie Gillibrand. After submitting multiple correspondences to the Department of Defense on June 6, 2016, a presidential inquiry into the treatment of Capt. Harrell was launched by the White House.

Between July 7 and July 11 Capt. Varno and Bobbie Davis (Nurse Case Manager) sent me three emails in which they attached "signature verification" link. I found this slightly strange as Capt. Varno, Bobbie Davis, and I previously exchanged more than 20 combined emails in which none required an "email /signature verification." On or around July 11, 2016, several of my associates stated that they had not received any emails from me and I was not able to receive emails from them. Upon seeking technical support from Yahoo, a technician confirmed that my personal email accounts mscharrell@yahoo.com and cassandraharrell95@yahoo.com were hacked. During the short conversation, technical assistance attempted to charge me a fee to remove the attack (I have my credit card statement). Later, the technicians advised me to disable the accounts.

By hacking my personal email accounts, the hackers were able to determine my advocates for Capt. Harrell. Mr. Ricardo Finney was one of my most frequently emailed supporters. By hacking me, the culprits were then able to send fake links which resulted in the demise of Mr. Finney's email communication.

Additionally, the same hacker used individuals to stalk my family and I. due to the level of the stalking; I filed a complaint with the Douglas County Sheriff's Department. I can provide the incident report number, descriptions, and images of the vehicles and people used to surveillance my home. Also, I can provide proof to show that when my internet IP was hacked, every device on my home internet service was compromised.

- Commented [G1]: Inserted: ,
- Commented [G2]: Inserted: five
- Commented [G3]: Inserted: ,
- Commented [G4]: Deleted:5
- Commented [G5]: Inserted: i
- Commented [G6]: Inserted: s
- Commented [G7]: Inserted: r
- Commented [G8]: Inserted: ere
- Commented [G9]: Inserted: seven
- Commented [G10]: Deleted:7
- Commented [G11]: Deleted:as
- Commented [G12]: Deleted:o
- Commented [G13]: Inserted: a
- Commented [G14]: Inserted: ance
- Commented [G15]: Inserted: assi
- Commented [G16]: Inserted: c
- Commented [G17]: Inserted: n
- Commented [G18]: Inserted: e
- Commented [G19]: Deleted:a
- Commented [G20]: Deleted:n
- Commented [G21]: Deleted:uppor
- Commented [G22]: Deleted:a
- Commented [G23]: Inserted: r
- Commented [G24]: Inserted: r
- Commented [G25]: Inserted: supp
- Commented [G26]: Deleted:adv
- Commented [G27]: Deleted:ca
- Commented [G28]: Inserted: internet service was ... [1]
- Commented [G29]: Inserted: d, every device on
- Commented [G30]: Inserted: k
- Commented [G31]: Inserted: my internet IP was ha
- Commented [G32]: Inserted: de proof to show that wh
- Commented [G33]: Inserted: ance my home. Also, I ... [2]
- Commented [G34]: Inserted: i
- Commented [G35]: Inserted: n
- Commented [G36]: Inserted: c
- Commented [G37]: Inserted: ;
- Commented [G38]: Inserted: i
- Commented [G39]: Deleted;
- Commented [G40]: Deleted:am
- Commented [G41]: Deleted:bie to

g. i-pod, cell phone, state issued work computer, wireless printer, bank accounts, etc...) I have adamant reasons, and proof that this continued attacked was launched my commanders located at Walter Reed Medical Center(Warrior Transition Brigade)

Should you need additional information, please don't hesitate to contact me. My information is listed below:

Cassandra Harrell

harrellmillerc@gmail.com

Kindest Regards,

Cassandra

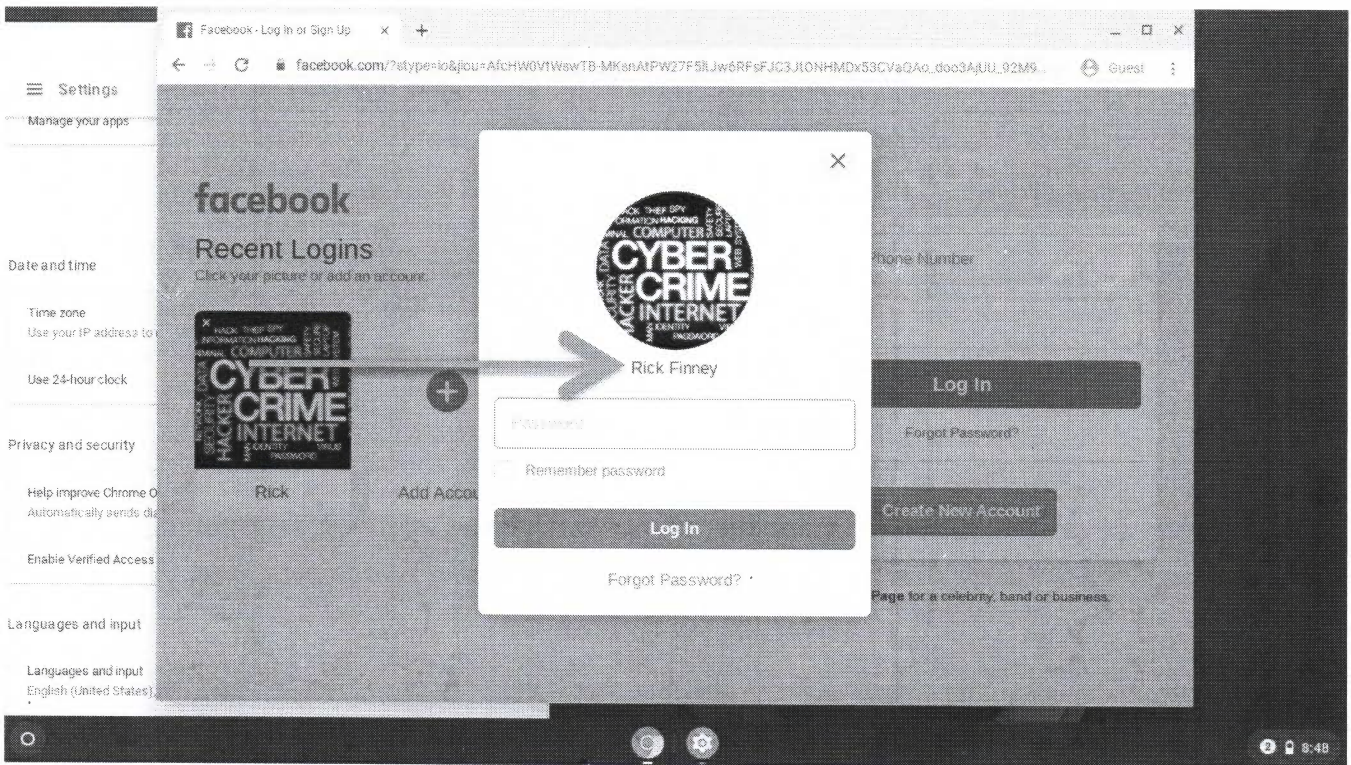
Commented [642]: Inserted: S

Commented [643]: Inserted: tate issued work computer, wireless printer, bank accounts, etc...) I have adamant reasons, and proof that this continued attacked was launched my commanders located at Walter Reed Medical Center(Warrior Transition Brigade)

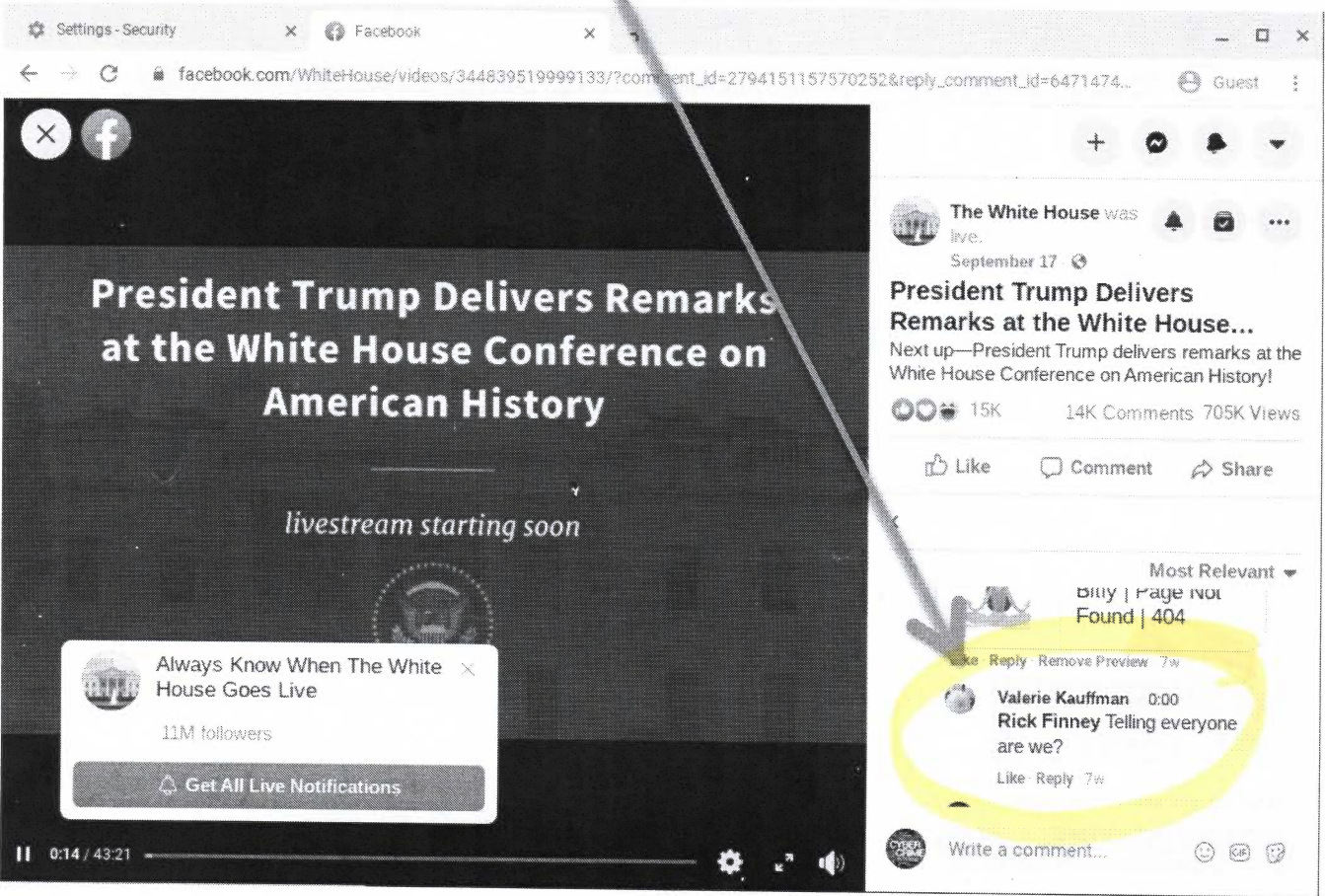
Commented [644]: Inserted: g. i-pod, cell phone,

Army cyber criminals hijacked my previous site at <https://www.facebook.com/rickfinney142>





One thing has persisted with the cyber criminals through my entire ordeal... Their penchant for sarcasm and attempts at psychological ploys. "Telling everyone are we"? Who is Valerie Kauffman? Why comment negatively about my situation? What's her attraction? Is she connected to Walter Reed with a trail back to the cyber criminals? Is she one of them?





Complaint Referral Form Internet Crime Complaint Center

No reply/No call back

Thank you. Your complaint was submitted to the IC3. Please save or print a copy of your complaint before closing this window. This is the only time you will have to make a copy of your complaint.

Victim Information

Name: Ricardo A. Finney

Are you reporting on behalf of a business? Yes

Business Name: Precision Photography

Is the incident currently impacting business operations? Yes

Age:

Address: 92-1206 Hookeha Place

Address (continued):

Suite/Apt./Mail Stop:

City: Kapolei

County:

Country: United States of America

State: Hawaii

Zip Code/Route: 96707

Phone Number: 8082559701

Email Address: nikon@precisionphotography.live

Business IT POC, if applicable:

Other Business POC, if applicable:

Description of Incident

Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.

On 6/17/22 I attended a cyber crime seminar in Kapolei, Hawaii attended by FBI Special Agent Roach-Vaden, head of the FBI Cyber Crime division at the Kapolei, Hawaii Field Office. I spoke briefly to Agent Roach-Vaden explaining I had filed multiple IC3 complaints and never received a reply. Agent Roach-Vaden explained the lack of a reply should not occur and said I should have received answers. I asked him for an appointment at his earliest convenience to be interviewed about my FBI IC3 submissions. Agent Roach-Vaden noted he had just relocated to Hawaii and would be unavailable since he would be settling in the next week. However he stated

he'd have one of his agents call me the next week. I left my business card with Agent Roach-Vaden. The week passed, I did not get a call. To date I have not received a call.

I am federal whistle blower seeking cyber crime victim assistance after receiving very sophisticated non-stop cyber attacks in retaliation. Please coordinate arranging a call to me from Agent Roach-Vaden or one of his agents as promised to schedule an interview about my FBI IC3 submissions and ongoing cyber attacks. I respectfully request a call to schedule an interview before 1700 EST time Wednesday, September 7, 2022. In addition to my IC3 submissions, I'd like to discuss investigating these two recent cyber attacks I received and report here:

I discovered two hacking incidents in my Apple laptop. Cyber criminals exploited the Apple remote access application Disk in the Mac operating system. The Disk application now connects to my network and gives connectivity to an address I can't determine. My computer has been illegally modified to have my network connect remotely to an unknown address. I have no idea where the hacked application goes online after it connects to through my network. Since the Disk app is embedded in the Apple operating system I can't erase the remote control app. I also cannot control it in any fashion.

Additionally, the Express VPN application in my Apple laptop is compromised. My computer has been reconfigured to require access to Mac Settings to enter an (unknown) password to install ExpressVPN. Without the password the software will not operate. In a clean computer the installation process is automatic. There should be no requirement during the installation process to access Mac Settings. There should be no requirement to enter a password to continue. All installation processes should be automatically populated with the only requirement being impressing clicks to advance through installation completion. In an 8/10/22 email, Express VPN validates the installation process should be automatic and should not require any access to Mac Settings.

The cyber criminals conduct successful attacks to disable my VPN and other software in my Mac and PC devices each time I attempt installation or try to use installed VPN software. I have four relevant letters from my computer technicians that validate different times my VPN and other software was hacked and disabled the same as now. Many other instances have occurred. However, this repeat incident in my Apple laptop with hacked VPN software is the first where the result of the compromise is readily evident to the eye in addition to being embedded in the operating system.

Honolulu Police Department Detective Thomas Iinuma has a case file with all the details described here.

Which of the following were used in this incident? (Check all that apply.)

- Spoofed Email
 Similar Domain
 Email Intrusion
 Other Please specify: Business Network
Intrusion/Hacking

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

[No response provided]

Are there any other witnesses or victims to this incident?

[No response provided]

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

Honolulu Police Department Detective Thomas
Iinuma (808) 723-3592
tiinuma@honolulu.gov Report #22-154047

Check here if this an update to a previously filed complaint:

Who Filed the Complaint

Were you the victim in the incident described above? Yes

Name:
Business Name:
Phone Number:
Email Address:

Digital Signature

By digitally signing this document, I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S.Code, Section 1001)

Digital Signature: Ricardo A. Finney

Thank you. Your complaint was submitted to the IC3. Please save or print a copy of your complaint before closing this window. This is the only time you will have to make a copy of your complaint.



Thank you. Your complaint was submitted to the IC3. Please save or print a copy of your complaint before closing this window. **This is the only time you will have to make a copy of your complaint.**

Victim Information

Name: RICARDO A. FINNEY
Are you reporting on behalf of a business? Yes
Business Name: Precision Photography Hawaii LLC
Is the incident currently impacting business operations? Yes
Age: [None]
Address: 92-1206 Hookeha Place
Address (continued):
Suite/Apt./Mail Stop:
City: Kapolei
County: Honolulu
Country: United States of America
State: Hawaii
Zip Code/Route: 96707
Phone Number: 8082559701
Email Address: raineer44@lionofjudah808.live
Business IT POC, if applicable:
Other Business POC, if applicable:

Description of Incident

Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.

As your records reflect, I am a federal whistle blower against Walter-Reed Military hospital. I continue to receive harassment, stalking on and offline, and computer and cell phone hacking in retaliation. Calls I made to (808) 824-9725 using my Verizon iPhone with number (808) 688-4897 stopped connecting through Google Voice after being illegally intercepted and blocked. Calls, texts, and voice messages on the same phone to other numbers connect problem-free. The owner of the (808) 824-9725 number is Mrs. Anna Odom from Kapolei, Hawaii who agreed to assist me through facilitating the investigation and exposure of targeted cyber attacks I receive in retaliation for my whistle blowing attempts. Cell phone logs reveal my device's network was flooded with hundreds of calls each hour of each day from 1/17/22 through 2/21/22 by events resembling Denial of Service attacks. I did not make these repeated calls. My communication with Ms. Odom has been blocked to prevent our interaction and resulting criminal disclosures. Cyber criminals stalk me online and disable my VPN programs and computers to prevent me from exposing their stalking and harassment because of my attempted federal whistle blowing. On 2/21/22 at 1420 I learned the Nord VPN program in my Dell desktop computer had been illegally accessed and disabled during a software restoration after the computer was hacked. I received the computer after it was serviced by Mr. Laine Kohama (808) 673-4749 from Gigaisland Computers in Honolulu. On 2/28/22, at 1420 Mr. Kohama confirmed the NordVPN program that had been installed correctly prior to being disabled. Additionally, four different VPN apps were blocked from connecting to my laptop and the computer was hacked to prevent any of the four different VPN programs saved to a USB thumb drive from installing into the computer. On 3/11/22 at 1830 I discovered the operating system in my Acer desktop computer has been changed to bypass the security password needed to block and unblock my Public, Private, and Domain firewall settings. My devices are illegally accessed remotely and software in the operating system or third-party applications are damaged or disabled in the background. On 3/11/22 at 1850, I discovered the printer function in my Acer desktop computer had been hacked and disabled. My combined business equipment losses as a direct result of cyber attacks in 2021 through 3/11/22 is \$11,350.25. The incessant hacking has prevented my wife and I from earning a living from our 3 computer-based businesses. On 3/16/22 I filed a very detailed compromised cell phone and computer cyber crime report with the Honolulu Police Department. I received cell phone and computer cyber attacks against all my networks hourly. Please investigate my claims immediately and stop the crimes committed against me.

Which of the following were used in this incident? (Check all that apply.)

- Spoofed Email
- Similar Domain
- Email Intrusion
- Other Please specify: Cell phone and computer hacking

Law enforcement or regulatory agencies may desire copies of pertinent documents or other evidence regarding your complaint.

Originals should be retained for use by law enforcement agencies.

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

raineer44@lionofjudah808.live
veteranlist@protonmail.com

Are there any other witnesses or victims to this incident?

Laine Kohama 808 673-4749

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

Lt Maddock Honolulu Police Department Police statment filed 3/16/22
amaddock@honolulu.gov

Check here if this an update to a previously filed complaint:

Who Filed the Complaint

Were you the victim in the incident described above? Yes

Digital Signature

By digitally signing this document, I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S. Code, Section 1001)

Digital Signature: Ricardo A. Finney

8/16/21



Complaint Referral Form Internet Crime Complaint Center

No reply/No call back

Victim Information

Name: Ricardo A. Finney

Are you reporting on behalf of a business? Yes

Business Name: Precision Photography Hawaii, LLC

Is the incident currently impacting business operations? Yes

operations?

Age: Over 60

Address: 92-1206 Hookeha Place

Address (continued):

Suite/Apt./Mail Stop:

City: Kapolei

County: Honolulu

Country: United States of America

State: Hawaii

Zip Code/Route: 96707

Phone Number: 8082559701

Email Address: 808vipphotography@protonmail.com

Business IT POC, if applicable:

Other Business POC, if applicable:

Description of Incident

Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.

My previous complaint filed today was incomplete. This is a resubmission.

I am contacting your again with a request to intervene and stop illegal cell phone wiretapping, phone software intrusions, and computer cyber crimes committed against me and my family I. The crimes are perpetrated in retaliation for my whistle blowing against the US Army as addressed in 9 prior IC3 cyber crime complaints sent to you since 2016. My family and I continue to suffer severe, around-the-clock retribution. Steadily increasing cyber attacks by members of the US Army or its agents against my family and I have rendered all my business and personal computers, tablets, and cell phones unsecured, unsafe, and in some cases, unable to be used. My business cell phone is illegally compromised with selected calls blocked, audio scrambled, and Internet pages hacked. I have forensic and other evidence to support this claim. The Army cyber criminals have used very sophisticated processes to breach my business network, infected my PC and Mac computers, and disabled these essential security and communication software programs and locations:

Malwarebytes Faronics Deep Freeze Spybot ebay Express VPN NordVPN
 mailbox.org Box.com Dropbox.com Microsoft Office 365 Suite
 Facebook Twitter MITM Guard (Blocks Man-In-The-Middle attacks)

Illegal Bluetooth transmissions the criminals used to compromise my equipment did not appear

in routine security scans run by my computer technician, Mr. Laine Kohama (808) 673-4749, and investigators from the State of Hawaii Department of the Attorney General Investigations Division. Discreet, unwanted Bluetooth connections were used to compromise my devices in a way identical to those not visible and thus unseen during visits I made to Apple computer stores seeking repair. I have operating system logs from the compromised computers that support my claim. These logs reveal malicious Bluetooth connections used to infect and disable my iMac laptop and desktop computers during repeated visits to the Apple stores

The cyber criminals have disabled several critical security software applications in my devices. One of the most critical items rendered unserviceable is my Virtual Private Network (VPN) software in my computers, tablets, and cell phone. They have disabled my VPN applications on the other side of my firewall allowing them to stalk me online with ease, then intercept and block my connectivity to web pages or Internet links they perceive as a threat to exposure or will allow me to download software I need for marketing use. They also hacked me by exploiting authentic, but unsecured http web pages.

In order to resolve this problem I have work remotely with my network engineer who has to establish a remote connection via a passcode which I cannot give on my secure phone. Even if I connect with my network engineer, the cyber criminals who know where I am online then attack my remotely connected computer. My engineer explained I have to connect remotely to see what is stopping me from reaching my VPN connection.

The email address of anyone I give a cyber crime evidence website link I posted online cannot connect as they are also stalked and blocked from connecting to my site to see the content. The cyber criminals compromised my Twitter and Facebook accounts to prevent my online postings.

Cyber criminals have disconnected the CD/DVD burner software in my Dell desktop PC. They disconnected my Brother laser jet printer from my Acer desktop PC computer. They compromised or completely disabled five Chromebooks, four Macs, three iPads, and six PC desktop and laptop computers. Each time I have my devices repaired, the sophisticated cyber criminals find a way to reacquire and infect or disable them. For example, after restoration five of my devices have been compromised since from mid-March through May 2021. The cyber criminals wrote malware in my computer that infects USB thumb drives when inserted. Earlier this month they blocked my access to my business website admin portal to prevent me from renewing my business website hosting.

The Army cyber criminals have hacked my personal Netgear router used for entertainment and installed blocks to prevent me from connecting devices. The criminals block selected phone calls and disable Zoom video meetings to prevent me from connecting with business and other contacts. They stalk me online and know when I log into Box.com and Dropbox.com cloud storage portals, then hack into my connection and erase evidence files I try to upload as fast as I post them. I cannot conduct secure online business banking or correspond online with other financial agencies as a direct result of repeated computer device compromises.

Through illegal phone surveillance the criminals listen at conversations I have with my network engineers in California and my local computer technicians. After listening and know what is planned, the cyber criminals attack and infect or disable my hardware. I have evidence to support this claim. I have to link with the engineer remotely to troubleshoot and resolve the hacked connection which leaves my computer open to another cyber attack.

My Hawaii state application for COVIT-19 pandemic unemployment assistance was delayed because I suffered identity theft. I filed theft reports with the state pandemic relief office and the Federal Trade

Commission. I am certain the crime was perpetrated by the same cyber criminals who continue to attack me. Being targeted by them, I know of no other source who would want to prevent me from receiving PUA payments by sabotaging my application through falsely applying in my name and using my social security number. These and other criminal incidents negatively affect my ability to resume operating my small business impacted by COVIT-19 and the cyber attacks. As a commercial photographer I am totally dependent on computers to complete my work. Of particular impact are the attacks on the engines of my livelihood, my business website and Microsoft Word processing and Microsoft Outlook email addresses. I can't communicate with prospective and established photography clients because our email communication has been blocked. I have evidence to support this claim.

Recent cyber attacks on Friday, August 6 and Monday August 9, 2021 that disabled my business email can be validated by Mr. Kohama who is examining my business computers to attest to the intrusions. Currently, he is examining my business computers to attest to the intrusions that now exist. He will also validate my computers were changed from proper installations he made previously. In each case the changes were malicious after the cyber criminals infiltrated my business network and hacked my devices after I received them back from Mr. Kohama. I have hired him to again provide factual documentation to prove my criminal damage claims.

I am attacked because the US Army wants to hide my persecution and the reason for the whistle blowing. The objective is to keep what has happened that I'm involved in silent and hidden. Ms. Cassandra Harrell, a fellow whistle blower, is victimized by identical crimes. I ask that you contact her to validate her circumstances and why I am being attacked:

(678) 891-9558 cassandraharrell@hotmail.com (601) 782-2092 mscyharrell@gmail.com

These are a few of the damaging cyber crimes that have been perpetrated against me:

bluetooth compromises: I have proof my devices were compromised through malicious Bluetooth connections unseen by Wi-Fi or software security scans. For many months my computer technician and I were unaware malicious Bluetooth connections were used illegally to compromise my devices. My \$2000.00 firewall does not detect Bluetooth signals.

no replies to email: I have examples of many business contacts whose communication abruptly stopped or did not reach me at all.

compromised iPhone: I have forensic reports that reveal compromises to my cell phones. The hacks include self-texting, delayed dialing, calls blocked with audio evidence, illegal GPS surveillance, and illegal voice mail transcription. I have filed dozens of police reports with the Honolulu Police Department

UPS to epoch times stolen: I have evidence revealing my whistle blower information sent via UPS to the Epoch Times newspaper in California was intercepted and stolen to prevent receipt. Follow-on submissions to the Epoch Times remain unanswered.

7mystolenappleid: I have evidence that reveals how my Apple ID was stolen and used through a cloned cell phone to wiretap my phone, along with evidence and witnesses proving my security software was attacked and disabled. I have evidence revealing four malicious connections made through phones owned by friends into my phone linking into my Verizon cellular network.

business site hosting renewal blocked: Cyber criminals block communication to my business website host asking to assist after cyber criminals blocked access to my admin portal so I could pay a hosting fee.

malwarebytes blocked: Criminals block my connectivity to Malwarebytes security software to prevent me from renewing my security software subscription and leaving me with no protection

against disabling cyber attacks.

My computer technician, Mr. Laine Kohama, is intimately aware of the dozens of computer, tablet, and cell phone repair and replacement support actions taken after each attack against me by the cybercriminals. He can attest to the volume and sophistication of the attacks, and to the more than \$53,000.00 I have spent fighting to stay online and not stay hidden. Mr. Kohama is aware of the various types of cyber attacks I have suffered, and the frequency of computer repairs I have referred to him. The criminal incidents negatively affect my ability to resume operating my small business impacted by COVIT-19 and the cyber attacks.

I was able to navigate online before the most recent attacks, but today I have no reliable, secure voice communication, am blocked by the cyber criminals from using my encrypted business email, and cannot operate my VPN software to defeat online surveillance and intrusions.

With no secure online capabilities or secure, correctly operating cell phone, I cannot continue to conduct my small business My cell phone was compromised after attempting to use for an eBay online financial transactions. Their retribution has effectively destroyed our livelihood, finances, and lifestyle. My wife and I have lost our computer-based small businesses and suffered over \$2.7 million dollars in damages as a direct result of the cyberattacks and cell phone control. I have financial records to support this claim.

I have had to cancel virtual medical appointments with the Veteran's Administration because I have no privacy on my cell phones and tablets.

Correspondence I sent to the Department of Justice in September 2020 intended for your action received a reply from the Army in January 2021. The reply indicating no action came from the same agency who continues to retaliate against me.

I have a 1000+ page forensic report, audio and video recordings, compromised physical SATA and SSD drives, infected USB thumb drives, firewall engineer reports, and cyber crime witness testimony to validate my claims of retaliatory criminal activity against me and my family. With over five years of assimilated on and offline files and folders, I have over 6 TB of evidence data compiled.

I have more information, however the available space in this area will not allow me to enter it.

Please intervene me without delay and stop the cyber crimes and illegal cell phone wiretapping and surveillance my family and I continue to be victimized by. Please have an agent call me at 808 255-9701 right away to arrange an interview and investigation of my eviden

Which of the following were used in this incident? (Check all that apply.)

- Spoofed Email
- Similar Domain
- Email Intrusion
- Other Please specify: Illegal cell phone intrusion,
computer destructio

Law enforcement or regulatory agencies may desire copies of pertinent documents or other evidence regarding your complaint.

Originals should be retained for use by law enforcement agencies.

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

[No response provided]

Are there any other witnesses or victims to this incident?

Mr. Laine Kohama, owner Gigaisland Computers, Honolulu, HI, (808) 673-4749

Mr. Ole Hartman, Western NRG Network Professionals, Camarillo, CA, (805) 658-0800.

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

Special Agent Sam Keliinoi, State of Hawaii Department of the Attorney General Investigations
Division 808 586-1240, no email available, reported on 8/16/21, no report number assigned

Lt Keieu, (808) 723-3703, no email available, latest reports files on 3/28/21, 4/9/21, 4/12/21, 5/10/21, 5/13/21,
5/21/21 HPD report #21-151824 46 prior HPD reports filed in 2020, 2019, 2018, 2017, and 2016.

Check here if this an update to a previously filed complaint:

Who Filed the Complaint

Were you the victim in the incident described above? Yes

Digital Signature

By digitally signing this document, I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S. Code, Section 1001)

Digital Signature: Ricardo A. Finney

Thank you for submitting your complaint to the IC3. Please save or print a copy for your records. ***This is the only time you will have to make a copy of your complaint.***

HONOLULU POLICE DEPARTMENT STATEMENT FORM

Report No. 21-151824

Statement of: Ricardo A. Finney		Classification:	
Address: 92-1206 Hookeha Place		Date of Occurrence: 8/8/21, 8/13/21, 8/16/21	
Age: 69	Date of Birth: 02/222/1952	Occupation: Commercial Photographer	
Res. Ph.:	Bus. Ph.: 808 255-9701	Employer: Self-employed	
Location of Interview: Kapolei Station			

Please give a detailed statement answering all of the following questions:

- | | | |
|--|--|---|
| 1. What DATE and TIME did it happen? | 5. WHAT happened? | 9. DID YOU IDENTIFY any suspects? Explain. |
| 2. WHERE did it happen? | 6. HOW did it happen? | 10. DID YOU IDENTIFY any weapons? Explain. |
| 3. WHO was involved? | 7. WHY did it happen (prior events/causes)? | 11. ... any property? Explain. |
| 4. What WITNESSES do you know of? | 8. ANY OTHER relevant information? | 12. ... any vehicles? Explain. |

The undersigned freely and voluntarily provides the following statement:

On 8/8/21 at 10:40 a.m. I discovered cyber criminals infiltrated my home business and reconfigured my Dell desktop PC so after startup the Skype for Business program initializes and opens without a command. This action is malicious. Skype was exploited previously to allow unwanted connectivity to damage another computer I own. My computer technician, Mr. Laine Kohama, (808) 672-4749, reconfigured the computer in response to a previous cyber attack that occurred on May 21, 2021. He will attest to the fact the malicious Skype configuration was not in place when he returned my computer after his installation. I enclosed a DVD that shows the compromise.

The malicious installation begins at the 1:02 mark. The DVD also includes a screen shot that validates the affected software on my computer. On 8/13/21 I received another cyber attack that compromised my Outlook email login process was compromised through exploited Microsoft scripts. I attached a screen shot of an email I sent to Mr. Kohama that explains the attack in detail. I also attached numerous links and references from Microsoft, Malwarebytes, and other security vendors that reveal the type of attack I was subjected to and the negative results.

I attached screen shots from Google searches that describe the scripts that downloaded to my operating system as undoubtedly malicious. This repeats a trend where the cyber criminals who attack me modify "normal" software in ways that do not appear in routine malware scans. On 8/16/21 received another cyber attack that disabled the the Firefox browser on my Acer desktop computer and configured the operating system in a way that presents reinstallation of the Firefox software. I attached a screen shot that shows registry entries titled "NoModify" and "NoRepair" which appear to be in place to prevent repairing or reinstalling the Firefox software. I've received the

I have read this statement prepared by Ricardo A. Finney which consists of this typed/handwritten page and 1 continuation page(s), and have been given the opportunity to make corrections thereon. I attest that this statement is true and correct to the best of my knowledge, and that I gave this statement freely and voluntarily without coercion or promise of reward.

Signature

Investigator's Signature

Date: _____

Time: _____

Date: _____

Time: _____

STATEMENT FORM CONTINUATION PAGE

Statement of: Ricardo A. Finney

Rpt. No.: 21-151824

same attack against my Chrome browser. As a result, I cannot access the Internet through either application. Cyber criminals infiltrated my home business network and disabled the printer function in my Acer computer. As I've noted before; the targeted cyber attacks and illegal cellphone wiretapping occur because I am a whistle blower against the US Army. Their objective is to keep the crimes involved with the whistle blowing and retaliation against my family and I secret and hidden. The cyber criminals blocked uploads revealing crime evidence I've attempted to post on Twitter and Facebook. As proven in audio clips I've provided to you, the cyber criminals block the audio on selected phone calls I've made on my cellphone to prevent me from communicating with selected agencies. They have prevented me from communicating with the Hawaii state Pandemic Unemployment Assistance office. The jamming continues. Because of COVID-19, the Veteran's Administration is conducting only virtual medical appointments. I will be blocked from meeting my medical appointments because my phones and doctors. I ask again that you contact witness Cassandra Harrell who will validate why I receive the sophisticated, targeted cyber attacks: (678) 891-9558 mschyharrell@gmail.com

My financial losses from the two disabled computer totals \$5,345.31. Without operable, secure devices I cannot retrieve receipts to print, nor can I operate my computer-based business. I've asked Mr Kohama to provide written validation attesting the current compromised state of my computer is different than the clean configuration he installed. I do not have the computer skills needed to complete the malicious installations and render my computers unsafe to use online. Both computers were repaired previously following cyber attacks that disabled them. I provided visual proof and witnesses who will validate my claims. All of my hacked devices are available for your inspection. Please investigate my claims without delay. I did not authorize anyone to access my computers. I wish to prosecute.

computers, and tablets are hacked and incapable of supporting secure, private health care communication

Signature

Investigator's Signature

Date: _____

Time: _____

Date: _____

Time: _____

September 4, 2021

Memo For Record:

In an attempt to conduct surveillance and block my Internet access, the Army cyber criminals have compromised all of my desktop and laptop computers and Apple iPads. They did these illegal acts to prevent me from exposing their crimes.

This is a list of my devices the cyber criminals have compromised over the past 5+ years:

Desktop PC's

1. Dell - Disabled Windows Defender security scan (cycles back to start without scanning)
Disabled Express and Nord VPN's/Will not initialize to allow online surveillance
Compromised my wired and wireless networks to conduct Man-In-The-Middle
(MITM)
attacks to read and block my email traffic..
Changed registry files to force malicious connections.
Changed the Remote Assistance setting to allow remote access to the computer.
Reconfigured the operating system to infect thumb drives through the USB port.
2. Dell - Disabled Windows Defender security scan (cycles back to start without scanning)
Disabled Express and Nord VPN's/Will not initialize to allow online surveillance.
Compromised my wired and wireless networks to conduct Man-In-The-Middle
(MITM)
attacks.
Changed registry files to force malicious connections.
Changed the Remote Assistance setting to allow remote access to the computer.
Reconfigured the operating system to infect thumb drives through the USB port.
3. Dell - Disabled Windows Defender security scan (cycles back to start without scanning)
Disabled Express and Nord VPN's/Will not initialize to allow online surveillance
Compromised my wired and wireless networks to conduct Man-In-The-Middle
(MITM)
attacks to read and block my email traffic.
Changed registry files to force malicious connections. Modified the operating system
so the Skype application opens on the desktop without a manual command. The cyber
criminals have made malicious connections through Skype.
Changed the Remote Assistance setting to allow remote access to the computer.
Reconfigured the operating system to infect thumb drives through the USB port.
4. Dell - Disabled Windows Defender security scan (cycles back to start without scanning)
Disabled Express and Nord VPN's/Will not initialize to allow online surveillance.
Compromised my wired and wireless networks to conduct Man-In-The-Middle
(MITM)
attacks.

Changed registry files to force malicious connections
Changed the Remote Assistance setting to allow remote access to the computer
Reconfigured the operating system to infect thumb drives through the USB port.

5. Acer - Disabled Windows Defender security scan (cycles back to start without scanning)
Disabled my Firefox browser rendering it inoperable.
Exploited two Microsoft operating system files used to compromise my Microsoft Outlook email login.
Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks.
Changed the Remote Assistance setting to allow remote access to the computer.
Reconfigured the operating system to infect thumb drives through the USB port.

Apple Desktops:

1. MacPro - Reconfigured the operating system to infect thumb drives through the USB port.
Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks
Completely disabled the device by infecting the operating system and blocking startup.
2. iMac - Compromised login process/Cannot backspace typing

Apple laptops:

1. MacBook Pro - Disabled Express VPN/Will not initialize to allow online surveillance.
Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks.
Reconfigured the operating system to infect thumb drives through the USB port.
2. MacBook Pro - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks.
Reconfigured the operating system to infect thumb drives through the USB port.

PC Laptop:

1. HP 17" - Disabled Windows Defender security scan (cycles back to start without scanning)
Disabled Express and Nord VPN's/Will not initialize to allow online surveillance.
Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic..
Changed registry files to force malicious connections.
Changed the Remote Assistance setting to allow remote access to the

computer.

Reconfigured the operating system to infect thumb drives through the USB port.

Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks.

Security scans revealed malicious rootkit changes and infections.

Reconfigured the operating system to infect thumb drives through the USB port.

Chromebook Laptops: (Cyber criminals infect new operating systems written to thumbdrives intended to overwrite their compromises. New laptops I purchased only lasted long enough to discreetly upload a few evidence files online before being discovered and infected)

1. Dell - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.
Reconfigured the operating system to infect thumb drives through the USB port.
2. Samsung - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.
Reconfigured the operating system to infect thumb drives through the USB port.
3. Samsung - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.
Reconfigured the operating system to infect thumb drives through the USB port.
4. Samsung - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.
Reconfigured the operating system to infect thumb drives through the USB port.
5. Samsung - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.
Reconfigured the operating system to infect thumb drives through the USB port.
6. Acer - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.
Reconfigured the operating system to infect thumb drives through the USB port.
7. Acer - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic.

Reconfigured the operating system to infect thumb drives through the USB port.

Chromebook Desktop:

Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic. Reconfigured the operating system to infect thumb drives through the USB port.

8. Lenovo - Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic. Reconfigured the operating system to infect thumb drives through the USB port.

Lenovo Laptop

1. Compromised my wired and wireless networks to conduct Man-In-The-Middle (MITM) attacks to read and block my email traffic. Reconfigured the operating system to infect thumb drives through the USB port.

Total: 19 computers compromised

Each time the PC and Apple computers were compromised my technician removed the infected hard drives and installed a new uninfected drive which was later infected. The cyber criminals wrote malicious data in rootkits that would not delete no matter even when the drive was erased multiple times.

I have nine SATA and five SSD drives that were hacked, removed, replaced, and stored.

Additionally, the cyber criminals compromised six of my iPhones and ten Android phones in the same fashion as my computers, and more.

Forensic examinations performed on some of my devices proved these claims.

The Army cyber criminals made repeated cyber attacks to prevent me from going online and exposing their crimes/whistle blowing.