

August 21, 2023

Mr. Ricardo Finney
92-1206 Hookeha Place
Kapolei, HI 96707
(808) 255-9701 (808) 582-8806
joshua1nine@lionofjudah808.live ricardof@mailfence.com finney808@proton.me

Aloha, Sir or Madam...

Mr. Ricardo Finney of Makakilo is a targeted federal whistle blower and cyber crime victim with a news story. Please conduct investigative reporting about corruption and collusion involving the Honolulu Police Department Criminal Investigation Division (CID) and the Honolulu FBI's Cyber Crime Division against Mr. Finney because of the whistle blowing which involved the abuse and mysterious death of a US Army soldier.

For nearly seven years Mr. Finney, his wife, and his granddaughter have been under illegal phone and vehicle surveillance, had dozens of computers infiltrated, hacked, and disabled, and had their cell phones illegally wiretapped, all done to keep the circumstances involving the whistle blowing silent. Although Mr. Finney has filed dozens of cyber crime complaints and reports with the FBI and HPD, neither agency has acted to catch the cyber criminals making the attacks in retaliation for the whistle blowing. By purposeful acts of omission they have and continue to allow the attacks to occur attempting to exhaust Mr. Finney's ability to remain online and expose the injustices hidden by the government agencies.

Members of HPD CID purposely ignored 36 cyber crime victim statements/reports Mr Finney submitted from August 2016 through July 2022 in response to devastating retaliatory cyber attacks. These statements included documentation submitted by Mr. Finney's long-time computer technician validating Mr. Finney's computers had been hacked. Documentation included an email from a security software vendor validating their software had been hacked. After failing to conduct any useful investigation of even one documented cyber crime report from the 36 submitted, under false pretenses HPD CID closed all of Mr. Finney's cyber crime cases permanently in October 2022 because he was "uncooperative" which is a lie.

Two months later HPD CID alleged to arrange a meeting between federal cyber crime officers and Mr. Kohama under the guise of "pursuing Mr. Finney's case to catch the cyber criminals". Mr. Finney was barred from involvement with the explanation "he will be contacted at a later date" which never happened. HPD CID said nothing to Mr. Finney directly before, during, and after communicating with his computer technician about the meeting, nor that all Mr. Finney's cyber crime cases had been permanently closed with "no further action taken".

As the only credible witness HPD CID allowed, Mr. Finney remains certain beyond any doubt his computer technician would have been second-guessed or outright stifled so his testimony could be invalidated as other witnesses had been. Considering ethics and integrity, eliminating

Mr. Finney from his own cyber crime case investigation two months prior doesn't correlate with scheduling a key witness interview two months later and where Mr. Finney, the victim, was barred from attending. Based on HPD CID's negative history and past encounters, Mr. Finney saw zero benefit in his technician's attendance at the interview. Sensing a set up, Mr. Finney asked his technician to decline the interview. The reasons for declining are attached.

HPD CID jumped on the opportunity to find an excuse to finalize all interaction with Mr. Finney and claim all cyber crime investigations were terminated and done. When Mr. Finney tried to reschedule the cyber crime validation interview with the other federal officers involved without HPD CID's involvement, all ignored him. The FBI won't answer any of my nearly 25 IC3 cyber crime complaints filed since 2016 through 2022 in another attempt to keep the federal whistle blowing matters silent and hidden. In the summer of 2022 Mr. Finney met with FBI Cyber Crime Special Agent Roach-Vaden of the Kapolei Field Office who promised a response to the cases but failed to do so. Special Agent Rubbelke in the same office ignored my emails.

Fighting cyber attacks with extra security to stay online and relevant is expensive. Since the cyber attacks destroyed Mr. & Mrs. Finney's computer-based businesses they have taken out four home equity loans for income over the years to stay financially solvent and to keep filing cyber crime complaints and reports. Mr. Finney's attempts to generate income using eBay, Craigslist, and other e-commerce platforms are blocked by the cyber criminals. HPD and FBI cyber crime reports Mr. Finney filed lie dormant and ignored. Please ask HPD to produce a single cyber crime case of mine that has been thoroughly investigated. You will find none.

Past cyber attacks and those that continue today are intended to take me offline to keep the whistle blowing matter silent and avoid a formal cyber crime referral to the FBI. The cyber criminals behind the attacks stalk Mr. Finney's on and offline activity. They read and block Mr. Finney's emails, texts, and faxes. The attackers intercept phone calls and written content Mr. Finney sends to print and social media, cyber security agencies, and whistle blower advocates.

The objective is to totally silence Mr. Finney. Evidence proving Mr. Finney's claims are here:

<https://www.hiddenfederalwhistleblower.com>

<https://bit.ly/7yearsofdeceit>

<https://bit.ly/cyberattacksupdate2>

<https://bit.ly/3LEINLX>

I attached a list of key contacts who will validate my various claims. I also attached a series of suggested questions to ask HPD and the FBI. Their answers, and lack of answers will provide further evidence my claims are factual. Please bring the corruption and collusion out of the dark into the light. Thank you for your time and consideration.

Mahalo,

Ricardo Finney

***“When you tear out a man's tongue you're not proving him a liar.
You're telling the world you fear what he has to say...”***

Key Contacts

Mr. Laine Kohama, Owner Gigaisland Computers

(808) 673-4749 laine@gigaisland.com support@gigaisland.com

Mr. Kohama validated numerous devices were/are compromised. He has been my technician for 6 ½ years - Clearly understands I'm targeted. He has seen the results of the cyber attacks personally many, many times since 2016

Det. Thomas Iinuma, HPD/CID

(808) 723-3592 tiinuma@honolulu.gov

Most recent officer to be dishonest, commit acts of omission, negligent, and exhibit other misconduct. Claimed to have a cyber crime 'person of interest' Should be no problem providing ID. ***I submit there is no one and his claim is a lie.***

Claimed to conduct thorough cyber crime investigations. Should be no problem producing five cyber crime statements with HPD/CID investigative findings, facts, conclusions, and determinations. ***I submit there is not one report he can produce***

FBI Special Agent Mitchell Rubbelke, Cyber crimes

(808) 566-4300 mrubbelke@fbi.gov

Refused to respond to emails, refused to schedule cyber crime validation meeting FBI refuses to respond to 26 IC3 complaints I've filed since 2016. Never answered my letter sent to the DOJ. DOJ refused my request to task the FBI to find and stop the cyber criminals. DOJ and the FBI ghosted me. Thanking me for my letter to President Trump ??, the Army responded to my 9/3/20 letter sent to Attorney General Barr four months later on the day President Trump left office by telling me I did not qualify under the military whistle blower regulations, directed me to call law enforcement, and informed me matters are permanently closed.

Dr. Cassandra Harrell, the soldier's sister: (678) 891-9558)

drharrell@gmail.com harrellmillerc@gmail.com

Sister of abused, deceased soldier. Fellow whistle blower and cyber crime victim
Cyber criminals block our connections to prevent communication

Pastor Gary Mason, the family pastor: (202) 531-8148
gmock70@hotmail.com shanaaz.mason@yahoo.com

Soldier's family pastor, 1st person knowledge about the soldier's abuse

Fellow whistle blower and cyber crime victim

Editor Sharon Rondeau, online newspaper editor ThePostemail.com

editor@postemail.com

(203) 987-7948

info@postemail.com

(860) 556-9392

Wrote many online stories over two years about the soldier's treatment and demise.
Wrote stories about the illegal surveillance, phone wiretapping, on and offline stalking,
device hacking, all purposely ignored by law enforcement.

Fellow whistle blower

Cyber criminals block our connections to prevent communication

Kelaghn Noy, Owner Armadillo encrypted cell phones in Canada

kelaghn.noy@armadillophone.com

(604) 218-0348

operations@armadillophone.com

(888) 861-4332, ext. 100

Phone, website and email access both ways intercepted, manipulated, or blocked by cyber criminals. Cyber criminals blocked the return of hacked encrypted phones via DHL Canada Canada to Mr. Noy for forensic examinations. Conducting an "investigation" after previously revealing he had no international jurisdiction, Det. Inuma claimed he repeated the same phone calls. That was the full extent of his "investigation". He then demanded I deliver the phones to him permanently for "safekeeping" (I did not). Please call Mr. Noy who will validate he has failed to reach me by phone and email. Cyber criminals block our correspondence

Cyber criminals block our connections to prevent communication

Joyce Kuo, News Editor The Epoch Times Newspaper

(626) 478-7753

Joyce.kuo@epochtimesca.com

Through illegal surveillance cyber criminals intercepted and stole my evidence shipment via an impersonator. The Epoch Times has my story for publishing consideration, just what the cyber criminals, the DOJ, FBI, and HPD *don't* want: Exposure. Cyber crimes for 7 years and whistle blowing gone viral.

Please ask Ms. Kuo if she tried to call me and reached voice mail or a busy signal, never speaking to me directly. Ms. Joyce Kuo is a news reporter for the Epoch Times, a non-left, non-right newspaper. Joyce works in California with a headquarters in New York. Per our last correspondence, she is waiting on go-no go from headquarters.

If anyone has tried, including Joyce, to contact me at the email addresses I provided, their email to me failed not by accident. The reply they received indicated their email bounced back stating my mine was a spam address, or my server was misconfigured and couldn't accept email, or my address was blacklisted, all generated from the US Army hackers who have stalked me for the past 7 years and are high alert trying to stop me from revealing their retribution and criminal actions. Please ask Joyce if she has tried to call me or if her headquarters has attempted to reach me by phone and failed, repeatedly

getting a busy signal. My phone is wiretapped and cloned. The Army cyber criminals control the receiving end of my phone. I can make a contact, but once the number registers in their cloned phone they see what I see, then block the number arriving to me using voice. Please understand the FBI, who has never investigated even one of the 27 FBI IC3 cyber crime complaints I've filed since 2016 is on the hook for answers.

I submit calls made to my phone were bounced and eventually stopped. In the seven months since I began corresponding with Ms. Kuo I never received calls or voice mail from anyone at the Epoch Times. I'm positive any calls made to me failed as well for the nefarious reasons I detailed.

Cyber criminals block our connections to prevent communication

QUESTIONS TO ASK HPD

(Not in event order)

For details about each question, please refer to <https://bit.ly/7yearsofdeceit> Go to “Links”

- Det. Inuma closed all Mr. Finney’s cyber crime cases stating Mr. Finney was “uncooperative” by not surrendering two encrypted phones Mr. Finney had purchased from Canada. Previously, Det. Inuma stated his local police force had no international jurisdiction with no claim on the devices, yet Mr. Finney was considered accountable for delivering and relinquishing his property purchased from Canada without reimbursement or compensation. He was penalized for not doing so. Why?

- Det. Inuma closed all Mr. Finney’s cyber crime cases stating Mr. Finney was “uncooperative” by not delivering devices for “safekeeping” and “inspection” by the set deadline. Mr. Finney disclosed Det. Inuma deceitfully neglected to disclose he was unavailable on the scheduled day and time and explained why. Since Det. Inuma was unavailable on the day and time he set, and he did not have jurisdiction to lay claim to the cell phones why was Mr. Finney considered uncooperative?

- Det. Inuma demanded Mr. Finney relinquish ownership of his two encrypted cellphones for “safekeeping”. Why didn’t HPD simply refer the international incident over to the FBI?

- Because of the constant hacking repeatedly referred to Det. Inuma in emails, Mr. Finney explained he needed additional time past the imposed deadline to have Mr. Kohama configure a computer with advanced security. Why did Det. Inuma ignore Mr. Finney’s notification? Why wasn’t Mr. Finney allowed additional time to have a protected computer placed online?

- Det. Inuma required Mr. Finney to produce six years of computer servicing administrative records before any crime investigations would start. Why was this requirement stipulated when HPD/CID left so many prior and current cyber cases unattended and not thoroughly investigated ?

- Det. Inuma claimed HPD’s responses to documented computer compromises were never based on opinions and guesses. Mr. Finney states this is not true. Who is correct?

- During his four-month interaction with Det. Inuma Mr. Finney was not allowed to pause and take a break from his sessions. During the 6 ½ years Mr. Finney filed cyber crime reports with various HPD officers, HPD officers went on sick leave, left for vacations, and went for months with no feedback, updates, or case decisions referred to Mr. Finney HPD. How do you account for the disparity in treatment? Why was Mr. Finney forced to continue with no break when HPD officers were not held to the same standard?

- Under the auspices of being a cyber attack assistance resource, Det. Inuma directed Mr. Finney to Hawaii Cares, a mental health organization. Why wasn’t Det. Inuma forthright and direct about his referral? Why did he feel the need to make a mental health referral for Mr. Finney after this had been an action included in a formal HPD complaint against his supervisor Lt. Maddock?

Lt Maddock claimed Mr. Finney was paranoid and imagining the compromises referred as cyber crimes?

- Why wasn't Det. Iinuma forthright and direct about his referral instead of masking it under a guise of direct cyber crime support?

- On 1/13/23 Det. Iinuma told Mr. Finney's computer technician that he had reached out to many businesses and individuals mentioned to him by Mr. Finney seeking validation cyber criminals hacked Mr. Finney's computers. Det. Iinuma stated all the businesses refused to provide validation cyber criminals hacked Mr. Finney's computers. What and who were all the many businesses and individuals Det. Iinuma reached out to?

- From the 30+cyber crime cases Mr. Finney submitted, how many were **thoroughly investigated** with **conclusions and final determinations**?

- Det. Iinuma permanently closed Mr. Finney's cyber crime cases 10/17/22 and terminated direct communication with him. On 12/8/22 Det. Iinuma notified Mr. Finney's computer technician of an "ongoing investigation" into Mr. Finney's cyber crime cases. Det. Iinuma reopened Mr. Finney's cases without informing or involving the victim, Mr. Finney. Det. Iinuma prohibited Mr. Finney's involvement. How was there a valid "ongoing investigation" of Mr. Finney's cases in Dec 2022 when Det. Iinuma permanently closed all of Mr. Finney's cases in Oct 2022 and stopped interacting one-on-one?

- The arrangements for attendees at the interview with Mr. Finney's computer technician, Mr. Kohama did not include Mr. Finney, the cyber crime victim. Why was Mr. Finney denied attendance at the interview with Mr. Kohama? Why wasn't Mr. Finney informed about, and included in the planned interview?

- In response to Mr. Kohama's request for Mr. Finney to attend the interview, Det. Iinuma explained Mr. Finney could (quote) "join at another time." What date was "the other time" to be when all cases were permanently closed on 10/17/22?

- Did Det. Iinuma inform the other interview attendees for the planned January 2023 meeting that he had permanently closed all of Mr. Finney's cyber crime cases in October 2022?

ADDITIONAL QUESTIONS TO ASK HPD/CID
(From files at <https://7yearsofdeceit> - Links - Attachment 12c)

Questions asked to the HPD/CID Commander - No reply given

1. Please explain why the video Mr. Finney captured from his computer's desktop reveals pages at the postemail.com Facebook website rapidly changing in a movie-like fashion instead of changing when clicked as normal.
2. Please explain why the unusual action noted was not considered fact or sufficient evidence of online stalking and illegal remote access into Mr. Finney's home business network.
3. Please explain why the video Mr. Finney provided from his computer's desktop revealing my Standard and Administrator accounts active during the same attempted login session was not considered fact or sufficient evidence of online stalking and illegal remote access into his home business network.
4. Two items Mr. Finney considered hacked are listed at one of his evidence sites, <https://www.bit.ly/380QUg8> Why are the events Mr. Finney referenced in Attachment 12c at the site NOT considered hacking but instead normal computer issues or spoofing by scam callers?
5. Concerning how Mr. Finney's HPD crime statements were handled overall, have HPD officers been directed from higher authority to **not** investigate Mr. Finney's HPD cyber crime statements, regardless of the content or evidence presented? If not, why weren't my Mr. Finney's cases **thoroughly** investigated with determinations, conclusions, and crime prevention solutions provided?

Question To Ask The FBI

- Since 2016 Mr. Finney has submitted over 30 FBI IC3 cyber crime complaints and letters to the Chief Operating Office at the FBI Hawaii field office and the Department of Justice seeking law enforcement intervention to stop sophisticated, daily cyber attacks. Evidence provided includes forensic, audio, video, and written evidence along with testimonies from witnesses who validated Mr. Finney's cyber crime claims. Among numerous interviews, Mr. Finney was seen by agents in California and Hawaii and most recently sent emails asking for intervention to a Hawaii-based FBI agent who continues to ignore him. In seven years not one reply has been sent or a phone call returned by anyone at the FBI at any level.

- The FBI has been, and continues to allow the cyber attacks made against Mr. Finney to continue uninterrupted ignoring the forensic, audio, video, and written documentation he has presented along with written testimony from computer engineers validating his devices have been compromised again and again.

FBI Reasoning: The FBI's lack of action in coordination with HPD has a purpose. Investigating cyber crimes committed against me ultimately uncovers facts surrounding the whistle blowing. All those who are complicit are counting on the hackers to attack successfully and take me offline permanently, or continue attacking until I can no longer afford the high costs for specialized online security and my connectivity is blocked.

Question: With the mountain of cyber crime evidence presented over such a long period delivered to you by Mr. Finney, why have the cyber attacks against him and his family been allowed to continue without investigations being conducted