

Global Financial Crisis: Blaming Hackers Coming to a Bank Account Near You to Steal Your Life Savings

By Joachim Hagopian

Global Research, March 27, 2016

Region: <u>USA</u>
Theme: <u>Global Economy</u>

Add one more way to lose all your life savings. Many of us have heard about the covert "bail-in laws" that already went into effect this year in Europe making theft of private bank account assets "legal" in this topsy-turvy world where chaos and high crimes rule the day. The precedent was set a couple years ago in Cyprus where private citizens woke up one day and found the money they believed was secure in their banks suddenly stolen by the banks. Despite the Treasury Department and MSM propaganda that the bailout cost taxpayers only \$21 billion, it actually cost Americans trillions in lost housing wealth, 9.3 million citizens lost their homes from 2005-2014 through foreclosure or short sale along with plenty of lost retirement funds and lots of lost jobs.

The untold misery and suffering of so many American people had insult added to injury when not one top financial executive ever faced charges but in fact were rewarded with obscene yearend bonuses. Already knowing the American public will not stand for another massive tax-supported bailout excusing the criminal banking cabal's gambling addiction for misusing their money that caused the 2008 housing bubble crisis, now the \$247 trillion in exposure to casino-generated debt derivatives created by those same bankster gangsters are manipulating governments to deliver deceitful backdoor thievery that will cause the next financial crisis to steal whatever savings they may still have left sitting unsecured in their bank accounts.

But this month yet another potentially equal red alert danger now lurks to steal all our money. This time it's supposedly neither the private Federal Reserve banksters nor our federal government gangsters. It's the criminal hacksters who gained access to central banks' digital assets and pulled off one of the biggest bank heists in history a couple weeks ago. I'm talking about the \$100 million grab of Federal Reserve money that managed to recover only \$19 million of its lost assets for a grand total theft of \$81 million, still making it among the largest bank robberies in history. On the day before US Empire's 2003 invasion of Iraq, per Saddam Hussein's instructions to his son Qusay, \$1 billion was taken from the Iraqi central bank. And in 2007 Dar Es Salaam Bank guards in Iraq lifted another \$282 million.

Of course these greatest bank heists pale in comparison to the conveniently lost trillions by US government officials' looting of Iraq and US taxpayers. On the day before 9/11 <u>Defense Secretary Donald Rumsfeld</u> announced that he and his still unaudited Pentagon couldn't account for \$2.3 trillion. Only hours later co-conspirator New York Trade Center lease owner <u>Larry Silverstein gave the "pull it" demolition order</u> to take down Building 7 an incredible 20 minutes after the <u>BBC repoter prematurely announced</u> it had already collapsed. And then of course Building 7 is where all the <u>Defense Department financial records</u> were conveniently housed. On top of all this, amazingly <u>Donald Rumsfeld</u>, Secretary of Defense at the time, has

the audacity to go twice on public record pretending he didn't even know Building 7 was destroyed on 9/11. If lying was a crime, Rummie would be sure to get the death penalty. Perhaps he and the other treasonous 9/11 conspirators in Washington and Israel eventually will get their due for perpetrating the most colossal crime of the century.

In any event here's what we know about the latest bank robbery. An <u>online digital typo error</u> prevented what would have become the biggest single bank heist in history at a whopping one billion dollars! The still at large hackers managed to navigate past all the security checkpoints of passwords and ID's to access the Bangladesh central bank's payment transfers. Overcoming this hurdle, the online bank robbers then made three dozen requests moving money from the Bangladesh bank to entities in the Philippines and Sri Lanka. The sophisticated cyber thieves were able to successfully transfer \$81 million to the Philippines but a simple misspelling of the word "foundation" as "fandation" held up the Sri Lanka transaction of about \$20 million to the NGO Shalika Foundation. Bank officials say that the routing bank – the nearly bankrupt Deutsche Bank – caught the misspelling error and asked for clarification from the Bangladesh central bank which then stopped the transfer. Reuters was unable to even find any information for the hackers' NGO Shalika Foundation that apparently isn't listed as a registered Sri Lankan non-profit organization.

The Bangladesh central bank holds an account at New York City's Federal Reserve for international settlements. The inordinate number of sudden requests made to transfer funds to private entities also tipped the Federal Reserve off into alerting the Bangladesh bank. It's believed that the total number of funds requested that were successfully stopped range from \$850-\$870 million. A rather sobering and even scary realization is had the hacker(s) properly spelled the word foundation, perhaps a billion dollars would have been stolen before anyone in the central banking system would have even caught on that they were duped by some mysterious anonymous cyber-criminal(s) who fortunately for them flunked English spelling class.

The \$81 million was deposited into four private accounts at the Philippine's Rizai Commercial Banking Corporation. Officials of the bank were grilled by the Philippine Congress, underscoring the weak links in finance safeguards worldwide, especially since the stolen money came from a US Federal Reserve account in New York. The high profile incident also exposes liabilities in the global anti-money laundering efforts. This opens the can of worms highlighted in recent years by HSBC Bank scandal with ties to the City of London caught red-handed laundering dirty drug and terrorist money that governments and the terrorism network profit from worldwide drug smuggling operations that have netted billions if not trillions. Sinister military research part of black ops programs is largely financed the drug money that our Western governments criminally generate. The corrupt global financial system is notorious for laundering money through the central banking cabal and mob casinos all over the world. That fact alone has allowed the hackers in this case to use the Philippine bank as its launderer. Legalized criminal secrecy of shadow governments globally enable transactions into the billions to be routinely covered up.

In response to this case the Filipino presidential frontrunner <u>Senator Grace Poe</u> recently stated:

The trend now in the world is having bank disclosures, not bank secrecy. This is to prevent also the funneling of money down to terroristic activities, drug cartels, etc. We should be one with the international community in preventing such activities.

Somehow I very much doubt that her current counterpart in America, the Republican front-runner Donald Trump would agree as his casinos have been linked to <u>organized crime</u> although he has managed to avoid indictment thus far. In any event, the Rizai Bank accepted the stolen money deposits and then <u>sent them to the local casinos for laundering</u> purposes knowing that the Philippine anti-money laundering law currently does not apply to casinos. In last week's televised congressional hearing in Manila the bank branch's customer service manager testified that he witnessed on February 5th after \$81 million was deposited at the bank the branch manager loaded near a half million dollars in a paper bag and drove away with it. He also claimed that the manager attempted to bribe him with a sum of over \$100,000. Meanwhile the incriminated branch manager's lawyer said he has emails proving that senior Rizai officers from the main office approved of the money transfer to the casinos.

Back in February 2013 a Philippine senator chaired the hearing and decision that amended the Anti-Money Laundering Act applied to casinos after hearing casino lobbyists tout that their country's casinos were rivaling other big Asian casinos and hamstringing them would only undermine the rising international competition that brought much needed revenue to the nation. So reluctantly he gave approval for casinos not to be covered by the law. Ironically that same senator is now tasked with investigating how the stolen \$81 million ended up moving through the Philippine bank to the casinos and then disappeared. The scandal has opened up a so called black hole in the world's banking security as well as bank and casino money laundering. The Bangladesh central bank governor and two deputy governors resigned last week. Meanwhile the money trail in the Philippines has grown cold once the \$81 million reached the casinos as the hackers may get away with their crime. Though security researchers have attributed partial blame to malware and a faulty printer, the bigger fault clearly lies in the corrupt global financial system itself.

This business of online hackers cracking cyber security systems is anything but new. In 2015 the Russian security firm Kaspersky Lab disclosed that an estimated total of \$1 billion has already been stolen by multinational hacking gangsters from up to 100 banking institutions around the globe just within the last two years. Last October a gang of cyber-criminals in Eastern Europe concocted a particularly virulent virus that infected bank records and drained £20m from UK bank accounts.

It's becoming an increasing threat to life as we know it as louder warnings of worse calamities to come have been bombarding the Western pubic in both mainstream and alternative news media. America's largest bank, JP Morgan admitted that last summer hackers attacked the bank records holding the names, addresses and email addresses of over 76 million households along with 7 million small businesses. That's over a quarter of the US population's personal information has already been compromised.

The elite of elite central banksters, the City of London policy head Mark Boleat said last fall that the next global financial crisis could make a huge bank and all its <u>asset holdings</u> <u>suddenly disappear</u> in an instant. In his words the bad guys will be:

[&]quot;... Destroying bank records and changing the amounts people have in their accounts," blowing up the financial system like a "neutron bomb" as "a bank will disappear, a national bank."

Since virtually every major act of terrorism in Western nations is <u>state sponsored by the Western government</u> intelligence community as the handlers of Muslim jihadist patsies, the latest Brussels airport bombing another case in point, even more easily planned and executed financial terrorism committed by the diabolically minded ruling elite could manifest as the next sudden global crisis blaming an anonymous gang of cyber world criminals for ripping off everything we have insecurely stored as digital bytes in our local banks. We could easily wake up one morning in the very near future and find that all our life savings have just disappeared overnight, and the crime cabal elite could just say "oops, sorry but it's just those bad guys who are apparently doing it to us again." For years the federal government has been planning on one of these type cyber-world attacks causing the next international crisis. With their deep state secrecy, who's to say that this incident was actually caused by some computer geek outlaws or the subhuman psychopaths that own and control the world. Regardless of "who done it," the catastrophic outcome's exactly the same.

Mainstream media and the banking industry are pointing the finger at a handful of hacking criminals, the lapses in cyber-security and the money laundering in the Philippines when the real culprit over and above all those smaller players is the global financial system itself. Again the banking industry is based on debt-based thievery with which the elites have enslaved the global masses for centuries, so why should so much commotion be made when a few anonymous hackers rip off America's central bank when it's been ripping the people off especially since 1913's Federal Reserve Act. The crumbling bankrupted global financial system protected by its bought and paid for international crime cabal that presently governs every Western nation is the culprit behind terrorism, war, impoverishment, disease and every high crime committed in this world. Granted hackers can wreak havoc on the globe's financial system, but clearly the bigger problem facing the citizens of this world is the tyrannical stranglehold the elite is imposing on the global masses.

Joachim Hagopian is a West Point graduate and former US Army officer. He has written a manuscript based on his unique military experience entitled "Don't Let The Bastards Getcha Down." It examines and focuses on US international relations, leadership and national security issues. After the military, Joachim earned a master's degree in Clinical Psychology and worked as a licensed therapist in the mental health field with abused youth and adolescents for more than a quarter century. In recent years he has focused on his writing, becoming an alternative media journalist. His blog site is at http://empireexposed.blogspot.co.id/

The original source of this article is Global Research Copyright © <u>Joachim Hagopian</u>, Global Research, 2016

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Joachim**

Hagopian

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca