cyberIdaho Finance Financial Innovation Lab

Emerging Technology Advisory Committee Report

An Offensive Strategy is Necessary

Fighting Growing Pig Butchering Schemes & Industrialized Cybercrime Operations Targeting Americans

Executive Summary

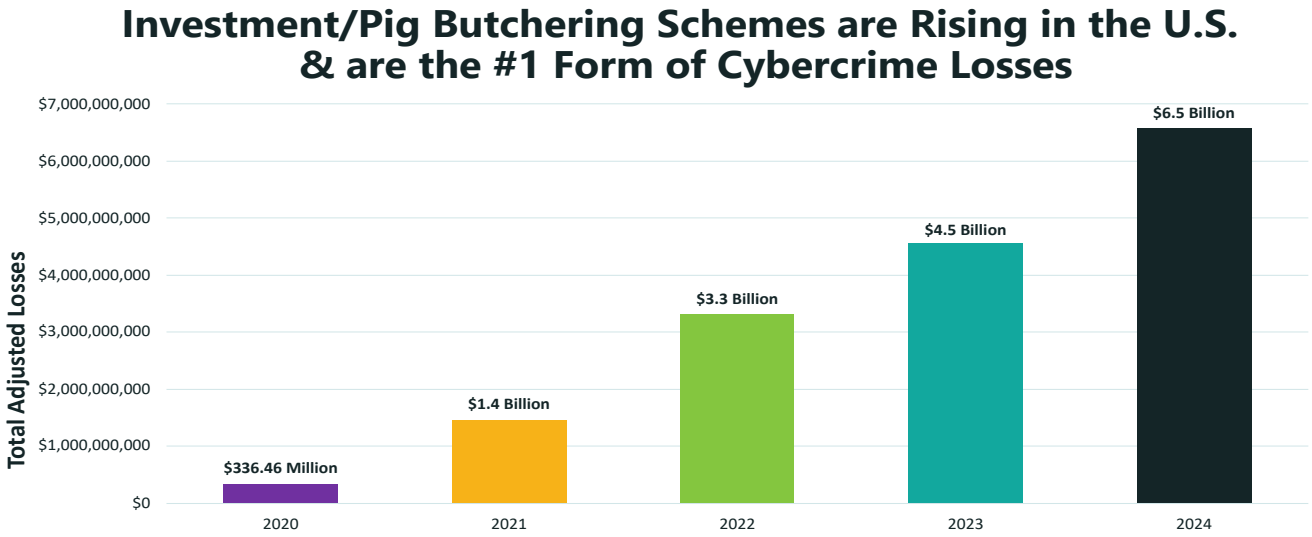
The emergence of large global organized cybercrime operations and compounds conducting pig butchering investment schemes is leading to surging financial losses for American citizens that requires a proactive offensive response from the United States (U.S.) government to dismantle these operations and better protect Americans from cybercrime. **Known American cybercrime losses increased to $16.6 billion in 2024 largely due to an over 1800% increase in losses from investment/pig butchering schemes since 2020.** A pig butchering cybercrime scheme combines elements of traditional investment schemes, romance/friendship scams, and cryptocurrency to fool innocent victims into sending funds to fake websites for fictitious cryptocurrency investments that are then stolen by illicit actors. Pig butchering schemes are popular with cybercriminals because it enables them to create an emotional relationship with victims that often leads to long-term continuous large deposits into their investment scams making them extremely profitable for bad actors.

The benefits cybercrime presents illicit actors in the form of profitability, scalable attacks, and global targeting combined with Americans becoming increasingly reliant on digital tools and services is motivating cybercriminals to organize and build dedicated physical industrialized cybercrime compounds to steal the wealth of Americans at scale. Since many cybercriminals conducting pig butchering schemes operate outside the reach of U.S. law enforcement in Asia, often with the help of complicit local governments, they are free to organize and develop large-scale cybercrime operations and compounds to target Americans with relative impunity. This means that U.S. cybercrime losses will continue to proliferate unless the U.S. adopts an offensive posture and strategy to attack these industrialized cybercrime compounds and pig butchering operations.

Increasing cybercrime and pig butchering losses highlight that organized cybercrime operations/compounds are currently overwhelming American defensive measures, which makes it essential for the U.S. to adopt a strategy that enables offensive cyber actions, provides necessary proactive authorities to government and private sector entities, and delivers key protections to potential American victims. A successful offensive cybercrime response strategy should include clear authorization from Congress and the White House for targeted cyber operations against industrialized cybercrime compounds and pig butchering operations, diplomatic pressure tools, primary and secondary sanctions, Department of Defense (DoD)/ Department of War (DoW) led offensive cyber operations, a letters of marque program, new proactive cybercrime prevention authorities and liability protections for financial entities, and tax liability protections for cyber and financial crime victims.[1] [2]

Pig Butchering Schemes are Driving Record Cybercrime Financial Losses for Americans

American financial losses from cybercrime reached another record high in 2024 and the number one form of cybercrime losses is from investment/pig butchering schemes, which makes the development of a strategy to counter these threats a priority for protecting the life savings of Americans. Investment/pig butchering schemes cost Americans $6.5 billion in 2024 accounting for nearly 40% of all known cybercrime losses in the U.S. last year.[3] According to the Federal Bureau of Investigations (FBI) Internet Crime Complaint Center's (IC3) metrics, investment/pig butchering schemes have grown exponentially since 2020 and overtook Business Email Compromise (BEC) as the costliest form of cybercrime in 2022 (see chart below).[4] [5] Currently, these schemes are also the top form of cybercrime losses in Idaho and are a driving force behind the state's 440% increase in known cybercrime losses between 2020 - 2024.[6]



Pig butchering is currently the most successful cybercrime scheme because it preys upon numerous psychological attributes (e.g., weaknesses, blind spots, and biases) that enable bad actors to build trust with victims over time, making it easy to convince them to send large sums of money for fake investments that cybercriminals then steal.[7] The term pig butchering originated in Asia and describes the "fattening up" of a victim by saturating targets with affection and/or constant attention to gain their trust before introducing fake investment opportunities and "slaughtering" the victims by stealing all their financial assets. Once trust is established with fake investing platforms showing phony profits to victims, the bad actors will continue to engage with their targets inducing them to invest more money by exploiting either their emotional connection or capitalizing on the excitement of wealth building. Once a victim falls into this trap, they will often lose hundreds of thousands or millions of dollars, and this is a major reason why pig butchering and cybercrime losses are proliferating.[8]

There is a clear correlation between pig butchering schemes and surging cybercrime losses for Americans. Due to the trusted relationships cybercriminals build with their targets in these schemes it is very difficult to protect victims strictly with defensive tools, which makes the adoption of a proactive offensive strategy essential.

Increasing Digital Technology Adoption, Jurisdictional Constraints, & Industrialized Cybercrime Compounds are Causing Pig Butchering Losses to Rise

The digitization of society along with a growing reliance on digital tools and services amongst Americans is creating an attractive opportunity for global cybercriminals to interact digitally with potential targets from jurisdictions outside the reach of U.S. law enforcement and safely profit from their pig butchering schemes. Currently, nearly 97% of Americans use the internet, 92% have access to smartphones, over 70% use social media, approximately 90% use financial technology, and over 80% interact via text/messaging applications, highlighting America's reliance on digital tools and services.[9] [10] [11] [12] As Americans increasingly depend on digital technology for everything from work and dating to entertainment and social interactions it creates the ideal environment for cybercriminals to target potential pig butchering victims from anywhere in the world. This makes it extremely difficult to effectively protect the public from pig butchering cybercriminals with a strictly defensive strategy, which makes the development of a complimentary offensive approach necessary to better protect Americans.

Cybercriminals have also found safe geographic regions in Southeast Asia to freely and successfully run their pig butchering operations without the fear of U.S. law enforcement disruption or legal accountability. Complicit nation states (e.g., Cambodia), areas of weak governance (e.g., the Golden Triangle that includes parts of Myanmar, Laos, and Thailand), and strategic tolerance (e.g., China's support for their Belt and Road Initiative and limited action against Chinese gangs) is providing cybercriminals with the buffer zones they require to organize their operations and steal the hard-earned money of Americans at will.[13] [14] [15]

The creation of dedicated organized physical industrialized cybercrime compounds within geographic safe zones in Southeast Asia are central to the scaling of pig butchering operations and the huge financial losses Americans are experiencing. These organized industrialized cybercrime compounds such as KK Park and the Crown Industrial Park (see photos in appendix A) have corporate-like structures in place with divisions of labor, modern technology stacks, security and financial operations, performance tracking/incentive systems, housing, and even food services built in with the single aim of committing cybercrimes.[16] [17] Many of these compounds are converted casinos, hotels, and office buildings that are staffed by human trafficking victims (over 300,000 trafficking victims are estimated to be conducting industrialized cybercrime in Myanmar, Laos, and Cambodia alone) who are forced to carryout pig butchering cybercrime schemes.[18] The infrastructure found in these industrialized cybercrime compounds is what allows these organized cybercrime operations to conduct pig butchering schemes at scale against Americans and is a key reason why U.S. cybercrime losses are exploding, making it necessary to target these facilities with offensive cyber actions and sanctions.

Pig Butchering Losses Will Continue to Surge Due to Industrialized Cybercrime Compounds & Emerging Technology Unless the U.S. Adopts an Offensive Mentality & Strategy

Cybercriminals will likely continue to target the wealth of Americans by building and developing more industrialized cybercrime compounds and implementing new emerging technologies into their operations that will intensify their pig butchering attacks and create large cybercrime losses for Americans. The U.S. is the wealthiest country in the world holding nearly 35% of global personal wealth and approximately $176 trillion in total household wealth, which will continue to make Americans prime targets for organized cybercrime and pig butchering operations.[19] [20] Cybercriminals conducting pig butchering schemes will also likely be given room to operate by complicit nation states, rebel groups, and strategic competitors such as China who stand to benefit from American wealth transfers.

The success of current pig butchering operations combined with the geographic safe zones organized cybercrime organizations are able to operate in ensures that illicit actors will build more industrialized cybercrime compounds to amplify their attacks and increase their profits at the expense of Americans. For example, Cambodia alone is currently home to nearly 350 known industrialized cybercrime compounds/sites highlighting that there are many more of these facilities targeting Americans operating throughout Southeast Asia.[21] The structure these compounds and sites bring enable large scale attacks that will lead to a substantial increase in American victim losses unless offensive actions are taken against them.

Cybercriminals and organized cybercrime/pig butchering organizations are implementing new emerging technologies and financial payment methods into their operations because they know law enforcement and oversight authorities will be a step behind and need to adapt. With more people depending on the internet for their everyday lives cybercriminals are now using artificial intelligence (AI) solutions to target victims at scale via

automated and personalized phishing campaigns, social engineering attacks, and deepfake attacks to further industrialize their crimes.[22] Bad actors are also incorporating new methods for exchanging value into their operations via cryptocurrency/digital assets that enables them to move illicit profits quickly and pseudonymously, making it difficult to track and seize these assets without necessary training, resources, and expertise.[23]

The fact that America remains the wealthiest country in the world and cybercriminals are scaling their attacks by building new industrialized cybercrime compounds and implementing new emerging technologies into their operations means that American pig butchering and cybercrime losses will continue to skyrocket until the U.S. adopts a proactive cohesive offensive strategy. It is also important that any strategy is realistic and seeks to protect potential American victims, especially seniors who are the number one demographic for cybercrime losses.

Policy Clarity, Offensive Cyber Actions, Sanctions, & New Stakeholder Tools/Protections are Key Pillars for an Offensive Cybercrime & Pig Butchering Response Strategy

The dramatic rise of pig butchering schemes that use industrialized cybercrime compounds to scale operations is driving the explosive growth in U.S. cybercrime losses and makes the development and implementation of a proactive offensive strategy essential for protecting Americans. Research shows that less than 1% of criminal financial proceeds are ever frozen or seized, which highlights the need for a more offensive approach to fighting cybercrime and safeguarding potential victims.[24] A strong offensive cybercrime response strategy should provide clear authorization for offensive cyber actions against industrialized cybercrime compounds and pig butchering operations, use diplomatic pressure tools and targeted sanctions, employ offensive cyber operations, incorporate private sector capabilities, properly equip financial entities with actionable cybercrime prevention authorities and legal protections, and codify tax relief for future cybercrime victims. To accomplish this goal the U.S. should take the following steps:

Policymakers Should Clearly Authorize Industrialized Cybercrime Compound Targeting – Congress should use its authorities (e.g., letters and hearings) to work with key Executive Branch stakeholders such as the U.S. Treasury Department and DoD/DoW to ensure they have the legal clarity and authorization they require to sanction and conduct cyber operations against physical industrialized cybercrime compounds and pig butchering operations. If there are any laws that require updating Congress should take legislative action to address these limitations.

The White House should also look to provide policy clarity for sanctioning and enabling cyber operations against industrialized cybercrime compounds by issuing an Executive Order that directs federal agencies to take more aggressive offensive actions against these compounds/pig butchering operations that are stealing the hard-earned money of Americans at scale. Without this policy clarity financial losses from cybercrime will continue to increase exponentially with limited repercussions.

Sanction Physical Cybercrime Compounds & Apply Diplomatic Pressure on Enablers – With policy and legal clarity in place the U.S. should impose primary and secondary sanctions on physical industrialized cybercrime compounds, cybercrime and pig butchering scheme operators (including their families and known associates), and any entities supporting or enabling these operations (e.g., complicit stakeholders providing technology, construction, and financial support etc.). The U.S. should use a mix of all sanctions options at its disposal including financial, travel, commercial, and others to target industrialized cybercrime compounds and punish bad actors who are benefitting by harming Americans.

The U.S. should also work with its allies to put more diplomatic pressure on state actors that are participating in and profiting from cybercrime, providing geographic safe zones, and/or are adopting strategic tolerance policies that allow industrialized cybercrime compounds and pig butchering operations to be successful (e.g., Cambodia, China, Thailand, Laos, and Myanmar etc.). The U.S. should collaborate with its allies to apply diplomatic pressure via sanctions, trade restrictions/export controls, foreign/military aid, security assistance, downgrading diplomatic relations, and other key levers that will cause these actors to take action against the industrialized cybercrime compounds and pig butchering operations that are stealing the wealth of Americans.

Authorize DoD to Conduct Offensive Cyber Actions Against Cybercrime Compounds/Operations – Once industrialized cybercrime compounds and pig butchering operations are identified and sanctioned, DoD/DoW should be able to conduct offensive cyber actions against their infrastructure and operations. DoD/DoW is in charge of conducting offensive cyber operations that disrupt, defeat, and deter adversaries in cyberspace through U.S. Cyber Command and the Cyber Mission Force, which makes DoD/DoW perfectly placed to take offensive cyber actions against these compounds and operations.[25]

Develop a Letters of Marque Program for Offensive Cyber Actions – As cybercrime and pig butchering operations continue to grow and scale the U.S. should enlist the assistance of the private sector in the fight against cybercrime by creating a letters of marque program within the federal government that authorizes offensive cyber operations. This program could be overseen by DoD to support their offensive actions, and it would leverage American talent and ingenuity by enabling key private sector stakeholders to target the industrialized cybercrime compounds and pig butchering operations that are leading to massive American cybercrime financial losses.

Empower Financial Entities with Freezing Capabilities & Good Faith Liability Protections – Digital asset entities and traditional financial service providers should be able to temporarily hold/block financial transactions without fear of legal liability when they believe a pig butchering/cybercrime scheme is occurring. New authorities similar to popular "Report and Hold" state laws should be granted to financial entities to protect Americans of all ages because once a bad actor controls funds/assets it is very difficult to get them back.[26] Bad actors in cybercrime schemes such as pig butchering and romance scams manipulate their victims into sending money, which often falls outside more traditional frauds involving unauthorized transactions that financial entities believe they can legally address.

The growth of cybercrimes involving manipulation is leading to an upsurge in lawsuits against financial entities for not taking proactive action, which means cybercrime and lawsuits will likely increase if entities are not given clear authority to proactively stop these transactions without fear of legal liability.

Congress Should Provide Tax Protections for Cybercrime Victims– Congress should codify in legislation that victims of cyber and financial crime do not pay taxes on any funds/assets that are proven to be lost/stolen. This proactive measure will help provide some small financial relief for cybercrime victims who often lose large sums of money and should not be a part of the U.S. tax base.

The creation of a proactive offensive cybercrime response strategy that adopts the above solutions will provide the legal clarity and tools necessary to better protect Americans and dismantle the industrialized cybercrime compounds and pig butchering operations that are causing record U.S. cybercrime financial losses.

Appendix A: Physical Industrialized Cybercrime Compound Examples

KK Park Cybercrime Compound (Myanmar)

Crown Industrial Park (Cambodia)

Endnotes

[1] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (refers to $16.6 billion in financial losses mentioned in the callout box).

[2] https://www.ic3.gov/annualreport/reports (the percentage change metric in the callout box is from IC3's annual reports between the years 2020 - 2024).

[3] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[4] https://www.ic3.gov/annualreport/reports (these statistics are taken from the IC3 annual reports between 2020 – 2024, which are also the documentation for the statistics shown on the page 2 chart).

[5] https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf

[6] https://www.ic3.gov/annualreport/reports (the percentage change metric for Idaho cybercrime growth is from IC3's state reports between the years 2020 - 2024).

[7] https://www.gowestit.com/the-psychology-behind-cybercrime-how-attackers-exploit-human-vulnerabilities/

[8] https://wordpress-1300524-4790431.cloudwaysapps.com/wp-content/uploads/about/press-releases/documents/2024/2024-DOF-PR-FLM-Tip-of-the-Week-Pig-Butch.pdf (documentation for pig butchering information in paragraph).

[9] https://datareportal.com/reports/digital-2024-united-states-of-america#:~:text=The%20state%20of%20digital%20in,percent%20of%20the%20total%20population

[10] https://www.theglobalstatistics.com/united-states-social-media-statistics/

[11] https://plaid.com/the-fintech-effect-2021-mass-adoption/

[12] https://www.localproject.net/docs/texting-stats/

[13] https://www.amnesty.org/en/latest/news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds/

[14] https://jacobin.com/2025/05/online-scam-industry-slave-labor

[15] https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf

[16] The term "industrialized cybercrime compound" used in this paper encompasses all physical scam compounds, scam centers, and scam sites.
https://www.dw.com/en/how-chinese-mafia-are-running-a-scam-factory-in-myanmar/a-68113480

[17] https://www.aljazeera.com/features/longform/2022/8/11/meet-cambodia-cyber-slaves

[18] https://www.voanews.com/a/report-southeast-asia-scam-centers-swindle-billions/7655765.html

[19] https://fortune.com/2025/07/14/how-many-millionaires-america-created-every-day-ubs-wealth/

[20] https://www.reuters.com/world/us/us-household-net-worth-rebounds-record-high-second-quarter-fed-data-shows-2025-09-11/#:~:text=Reuters%20Plus,US%20household%20net%20worth%20rebounds%20to%20record%20high%20in%20second,in%20wealth%2C%20Fed%20data%20showed

[21] https://humantraffickingsearch.org/wp-content/uploads/2024/10/Cambodia-CTIP-Factsheet-OSO-22OCT2024.pdf

[22] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[23] https://www.cyberdefensemagazine.com/why-do-hackers-love-cryptocurrency/

[24] https://www.interpol.int/News-and-Events/News/2022/FATF-and-INTERPOL-intensify-global-asset-recovery#:~:text=13%20September%202022,and%20requiring%20lengthy%20international%20cooperation

[25] https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/

[26] https://www.finance.idaho.gov/wp-content/uploads/2023/09/Senior-Fraud-and-Financial-Exploitation-Prevention-Report-2.pdf