WRITTEN TESTIMONY

OF

Erin West

Founder and Chief Executive Officer

Operation Shamrock

Former Deputy District Attorney (26 years)

Santa Clara County, California

BEFORE THE

HOUSE SELECT COMMITTEE ON STRATEGIC COMPETITION BETWEEN THE UNITED STATES AND THE CHINESE COMMUNIST PARTY

ON

Crime, Corruption, and Power:

CCP-Linked Transnational Criminal Organizations

and the Rise of a Distributed Threat to U.S. National Security

May 19, 2026

Washington, D.C.

I. WHO I AM HERE FOR

Chairman Moolenaar, Ranking Member Khanna, and distinguished Members of the Select Committee, thank you for the invitation to testify, and thank you for the work this Committee has now placed on the public record.

My name is Erin West. I spent 26 years as a deputy district attorney in Santa Clara County, California, on the REACT high-tech crime task force, and became one of the first local prosecutors in the country to specialize in cryptocurrency-enabled fraud. I left the courtroom to found Operation Shamrock, a 501(c)(3) nonprofit coalition of more than 2,000 law enforcement professionals, financial institutions, technology companies, and victim advocates, organized around a single mission: educate, mobilize, and disrupt the transnational criminal networks responsible for the scamdemic.

I have testified before the House Financial Services Subcommittee. I have submitted a statement to the Joint Economic Committee. I have briefed the National Security Council, congressional offices, federal agencies, state regulators, and federal prosecutors. I have traveled to Cambodia, Thailand, Myanmar, and the Philippines five times in the last three years to walk through the buildings where this crime is executed. I have worked alongside Shakilu, a Ugandan trafficking survivor who escaped a Cambodian scam compound and has since returned home. I host the Stolen podcast. I have spoken to more than 15,000 people about this crisis in a single year.

I am not here as a witness describing a distant problem. I am here on behalf of the people who will never get a seat in this room.

I am here on behalf of Chris, a single father in Massachusetts who lost ninety percent of his retirement to a fake girlfriend on Facebook and a fake trading platform whose only difference from the legitimate one was a doubled letter in the URL. I am here on behalf of Cristy, a university administrator in the Southeast who fell in love with an AI clone of a celebrity she had never met. I am here on behalf of Don, a retiree in Florida who lost more than half a million dollars and then traveled at his own expense to Singapore, Laos, and through Chinese provincial police to identify the kingpin who took it. I am here on behalf of Mary, a paralegal in Wisconsin who built a one-and-a-half-pound forensic evidence packet against the West African network that scammed her after the FBI never returned her call. I am here on behalf of Shakilu, a Ugandan trafficking survivor who escaped a scam compound in Cambodia and is now home. I am here on behalf of Mwesezi — a Ugandan gospel artist known to his fans as Small Q — who survived four days hung by handcuffs in a Burmese "dark room," watched a man die in front of him, stole an iPhone to alert his family, and is now releasing an album called *Back from Burma*. I am here on behalf of three fathers in Michigan, California, and Maryland whose children only learned why they took their lives by going through their digital lives after the fact. And I am here on behalf of every American constituent in every district represented at this dais who is being targeted today, right now, while we sit in this room.

I have read the Committee's report. The diagnosis is right. This is not Beijing issuing daily marching orders to scam compounds. It is something more dangerous and harder to dismantle: a criminal ecosystem the PRC tolerates, protects when useful, and allows to externalize enormous harm onto Americans. The Committee has correctly named what this is. The question is whether Congress will match that diagnosis with action.

I have been yelling about this for four years. In the twenty months since I last testified in person, tens of billions of dollars more have been stolen from American households, tens of thousands more people have been trafficked into compounds to do the stealing, and the compound infrastructure — far from being dismantled — is relocating, expanding, and hardening into terrain designed to be impossible to reach.

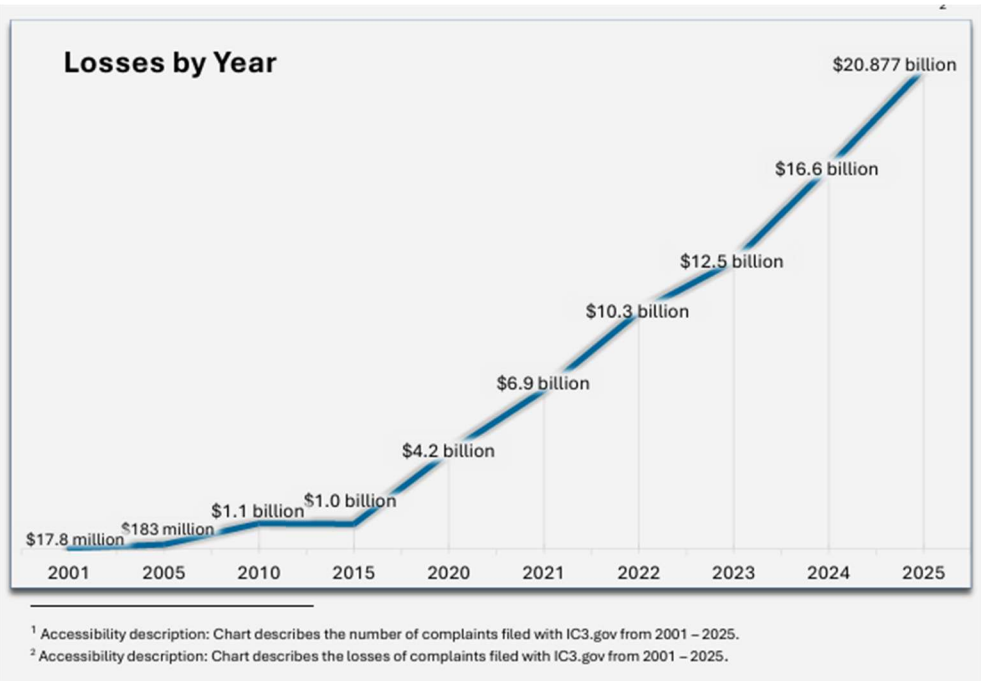
Don't wait another day.

II. THE SCAMDEMIC IS AN ECONOMIC EMERGENCY AIMED AT AMERICANS

I call this the scamdemic. Not for rhetorical effect, but because the word captures what is happening: a mass-casualty financial event spreading household by household, decimating savings, destroying retirement security, and transferring generational wealth out of the American economy at a scale that demands a national response.

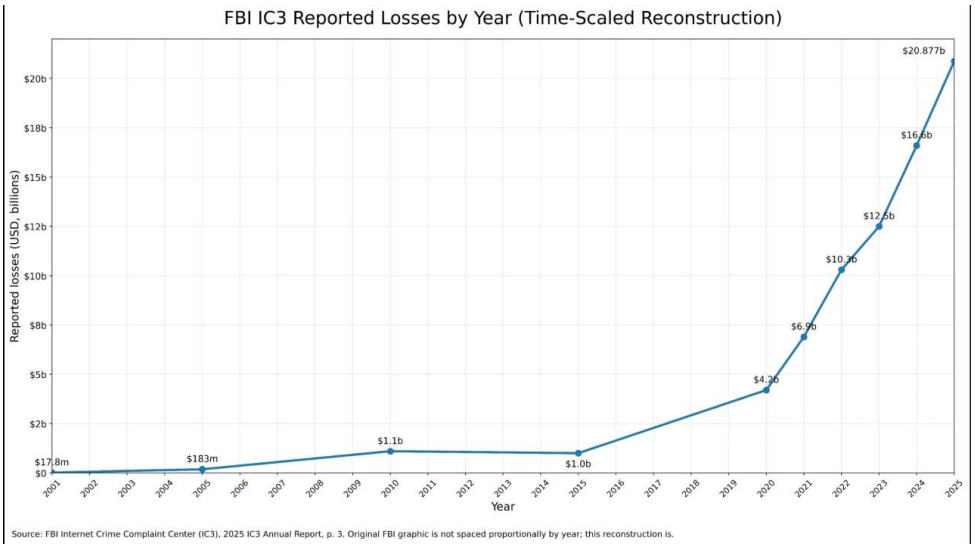
The FTC's 2024 Consumer Sentinel Network Data Book recorded $12.5 billion in reported fraud losses — a 25 percent increase over 2023, with investment scams accounting for $5.7 billion. Among older Americans, reported losses skyrocketed from $600 million in 2020 to $2.4 billion in 2024 — a three hundred percent increase in four years.

The FBI's 2025 Internet Crime Report, released this spring, confirms the trajectory has not bent. It has steepened. Total reported losses climbed to nearly $21 billion, with investment scams once again the single largest category.



[Insert: FBI IC3 2025 chart]

The graphic above, as supplied by the FBI, actually softens the curve. When the losses are spaced proportionally by year, the line is not a curve. It is a near-vertical climb.



The U.S. Department of the Treasury has assessed that Americans lose more than $10 billion annually to Southeast Asia–based scam compound networks alone. This Committee's report cites that number. I would offer it is conservative. Pig butchering victims do not report at anything close to one hundred percent — the shame of being deceived in love, layered with the shame of financial loss, is exactly what the criminals count on to suppress reporting. If we are seeing $10 billion at the visible end, the actual harm is multiples higher.

This crime exploded because it became the highest-yield, lowest-risk criminal enterprise in modern history. Long-distance fraud against Americans pays better than narcotics, runs on infrastructure designed for legitimate commerce, and faces enforcement that is fragmented across more than a dozen U.S. agencies and almost nonexistent abroad. The criminals understood the economics before we did.

That wealth leaves the American financial system and does not come back. It funds compound construction, militia protection, elite patronage networks, and — as the Committee's report and my own field observations confirm — strategic infrastructure that directly threatens U.S. interests.

This is not consumer fraud. It is systematic capital extraction at war-level scale. And it is not stabilizing. It is accelerating.

III. THE PEOPLE I AM HERE TO REPRESENT

Numbers can numb. Names cannot. Allow me to put faces to the data.

Chris. Chris (pictured above with his sons) is a divorced single father from Massachusetts. He served as an Army officer. He raised three sons. He became a grandfather in September 2024. He was four years from retirement.

In November 2024, a beautiful blonde woman with a German accent reached out to him on Facebook. He was skeptical. He pushed back. He asked for a video chat. She delivered one. She looked exactly like her photos. He let his guard down. Over the next several months, she introduced him to cryptocurrency,

walked him into a fake trading platform — a clone site whose URL differed from the real CoinMarketCap by exactly two letters — and pulled him into his IRA. When the platform demanded a payment to "open a large volume channel" to release his withdrawal, a man with New York plates showed up at his front door to collect cash.

Chris lost ninety percent of his retirement.

His local police told him they did not have the resources to help. He filed an IC3 report and never heard back. The Secret Service told him his loss was too small to prioritize. The Massachusetts Attorney General's office traced his money to an exchange in the Seychelles and could go no further. The fake profile that appeared on his video calls is, as of this writing, still active on Instagram. Chris has reported it repeatedly. Meta has repeatedly responded that she does not violate community standards.

Chris is the everyman victim of this crime. He is also a witness to the structural failures at every level of the U.S. response — local police without the tools, federal agencies without the capacity, platforms without the will. Chris did not get the opportunity to sit in this seat. He sent me his story so I could.

Cristy. Cristy is a university administrator who relocated to the Southeast in January 2025 to be near family. She made her Instagram profile public for one week to support her teenage niece's basketball contest. During that week, she commented once on the official Instagram page of comedian Matt Rife. That single interaction is what the criminals built on. A woman calling herself "Meredith" reached out, presenting as Matt Rife's PR representative. A reply from "Matt" followed — including a voice message in what was, beyond any doubt, his voice. It was an AI clone. Over six months, "Matt" walked Cristy into legitimate Coinbase and Kraken accounts and a fake portfolio that she watched grow. For the first time in her life, she felt financially safe. She purchased a property. She funded a remodel. Then "Matt" introduced his "financial planner," Brian. When she tried to withdraw, Brian asked for her ID, her Social Security number, and her passport. The real Matt Rife had performed in New York the week before. A close friend told her she was being scammed. Cristy looked her oldest friend in the eyes and said: *if I am being scammed, it was worth all the money I lost.* That moment captures what these criminals are actually selling. Not investments. Not love. They are selling an experience of being seen and heard, calibrated so precisely to a victim's life that the victim does not want to let it go even after the deception is exposed. That is the level of operational craft the United States is up against.

Don. Don is a retired engineer from St. Augustine, Florida. He was scammed in 2022 by a woman who appeared as a friend of a friend on Facebook and walked him onto a fake crypto trading platform that emptied his wallets. Don lost more than half a million dollars — money set aside to build a house. His local police told him crypto was not their area. The Secret Service in Jacksonville recovered approximately $29,000 — a fraction. The rest had moved to OKX and Binance overseas, where the agent told him, in essence, his case stopped.

Don did not stop. A private American citizen with no badge, he arranged for a police friend in Texas to formally request KYC information from OKX, which produced full identification on two Chinese nationals. He traced the money through a Singapore exchange to IP addresses in Vientiane, Laos. He flew, at his own

expense, to Singapore and Laos to file police reports in person. He spent approximately $40,000 on a Chinese law firm that worked with provincial police in Shandong. Through that channel, he obtained the name and passport number of a Chinese kingpin running scam compounds and a money-laundering ring spanning Burma and Laos — a kingpin Interpol had previously located in Laos and not detained. Singapore declined. Laos took the report and never acted on the IP addresses.

I told Don, when he walked me through this work, what should already be obvious to this Committee: imagine what you could have accomplished with a badge and a gun. Don did the investigation the federal response was not yet built to do. He named the Chinese nationals. He named the kingpin. He delivered an evidentiary record that would be the envy of most federal task forces.

Mary. Mary (pictured above) is a paralegal in Wisconsin who met a man on Plenty of Fish — a property of Match Group — in August. Over three months, she lost more than $100,000, withdrawn from her bank in twenty-four separate cash transactions of up to $15,000 each and fed into Bitcoin ATMs at Wisconsin gas stations. While Mary was being scammed, the same photographs were running on at least eight other Plenty of Fish profiles within a 200-mile radius of her home — and on at least seventeen additional fake profiles across other platforms — actively targeting other people in her time zone, in real time.

When Mary realized what had happened, she did something almost no other victim does. She did not break off contact. She stayed engaged with the criminals for three more months — to gather evidence. She sent them Grabify tracking links and harvested their IP addresses, which traced to Nigeria and Ghana. She built three forensic reports: a digital metadata analysis using AI; a physical evidence report on a fraudulent $850,000 check the criminals mailed her from a money mule address in San Jose, California; and a full investigative report. She sent a pound and a half of documents and a zip drive to Nigeria's Economic and Financial Crimes Commission and Ghana's Economic and Organized Crime Office. She received a personal response from the Executive Director of Ghana's EOCO within twenty minutes of his receiving the package. Through cooperation between local Wisconsin law enforcement and Binance, she has obtained the names of four Nigerian suspects from the cash-out wallets.

When the FBI did not respond to Mary, Mary built the case herself. She submitted policy recommendations that contributed to the March 6, 2026 Executive Order. She documented gaps in Wisconsin's cryptocurrency ATM regulation that became a bill signed into law by Governor Tony Evers on April 9, 2026. She is acting as a liaison between her local police officer and international law enforcement. The question Mary asked me, plainly, is the question this Committee should hold onto: *Why is it that in the United States in 2026, victims have to solve their own crimes?*

Don and Mary are extraordinary not because of what they lost, but because of what they did after. They built investigations the federal response was not yet resourced to build. They identified suspects on three continents the federal response did not identify. That is the indictment.

Six more faces, briefly. A retired high-school drama teacher I spoke with last fall lost her entire life savings, was talked into mortgaging the home she owned outright, and now works a sixteen-dollar-an-hour job at age seventy to avoid bankruptcy. I have spoken with the adult children of three different men — in Michigan, California, and Maryland — who took their own lives after being victimized in pig butchering schemes. Their families did not know why their fathers had died until they went through their digital lives and pieced it together after the fact. A fifteen-year-old boy in the Midwest was extorted through compound-traced sextortion and took his own life. International Justice Mission has now traced 493 confirmed child sextortion cases and more than 18,000 additional reports to the same Cambodian, Burmese, and Lao compounds draining American retirement accounts. The same infrastructure. The same enemy.

These are a few of the faces of tens of thousands. The point is not the volume; it is the pattern. The victim seeks help. The system fails them. Some, like Don and Mary, do the work themselves. Most do not have the time, the resources, or the resilience left to try. The money is gone either way.

IV. WHAT I HAVE SEEN ON THE GROUND

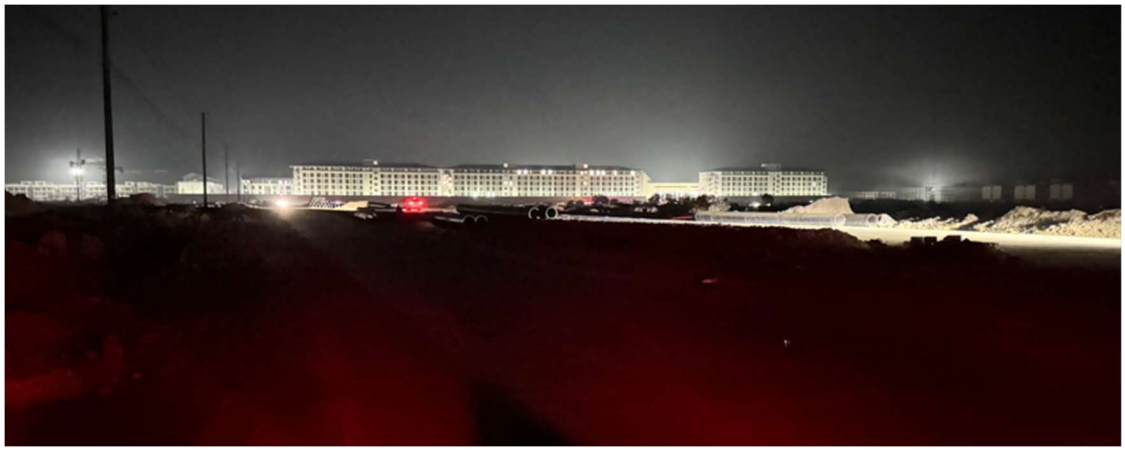
The Committee's report concludes that the criminal ecosystem in Southeast Asia is no longer concentrated in a handful of casino towers. It is distributed, embedded in local political economies, and increasingly hardened against intervention. I want to put primary evidence in front of this Committee that confirms each of those claims.

Sihanoukville, February 2025. I traveled to Cambodia with journalists Nathan Southern and Lindsay Kennedy of the Eyewitness Project expecting to see the massive compounds of Sihanoukville. I was not prepared for what I found everywhere else. Over a thousand miles of driving, we documented compound after compound — multi-building facilities behind two-story cement walls topped with razor wire, single controlled-access gates, bars on the windows. In cities. In rural areas. In corn fields and dirt patches in the middle of nowhere. Under construction. Everywhere. Sihanoukville's Chinatown is the size of a college campus, housing eight people to a room behind walls built not to keep outsiders out but to keep workers in. USIP and UNODC have estimated that revenue from the scam industry comprises more than forty

percent of the combined GDP of Cambodia, Myanmar, and Laos. In these countries, the compounds are not the margins of the economy. They are the economy.

Phnom Penh and Mansion 8, February 2026. I returned a year later with one question: is the crackdown real? In Phnom Penh, the surface looked genuine. One Prince building, where Cambodian police had blocked me from filming on my first trip, now had its gate down. I walked into an abandoned compound, waved through by a guard. Fine schedules were still posted on the walls — three hundred dollars for touching the air conditioner, one hundred dollars for misspelling a word. The rooms where scamming was conducted had metal doors that bolted from the outside, so workers were locked in while they worked. I saw green-screen walls, suggesting workers had been forced to impersonate law enforcement officials, possibly U.S. federal agents, on video calls. Every mattress in the compound was stacked in two rooms, ready to be placed back on beds. Thousands of chairs were stacked and waiting. This was not a closed business. It was a business on pause.

Three hours from Phnom Penh, on a dirt road near the Vietnamese border, we made a discovery. We had set out to find one compound, but out of our peripheral vision we noticed a massive set of buildings lit up like an NFL stadium, later identified as the Ace of Spades compound. We found a city under construction — four brand new distinct compound structures not yet visible on Google Maps, one of them at least a half-mile long, adjacent to a concrete factory, raw materials staged, road grading, and lighting infrastructure already in place.



[Photo: Ace of Spades compound, Cambodia, taken by Erin West, February 2026]

The Cambodian crackdown is a sleight of hand. The visible compounds are being cleaned up for the cameras. The industry is moving — to more remote terrain, less accessible to journalists, better defended, and at a scale beyond what any conventional law enforcement raid could address.

The supply side: Shakilu and Small Q. This Committee's report devotes substantial attention to the trafficked workers who are forced to do the scamming. I want to put two of their names on the record.

[Photo: Shakilu and sons, Uganda, April 2026]

Shakilu is a Ugandan national who was trafficked into a Cambodian scam compound. After contract work in Qatar ended, he and his brother started a small juice business at home in Uganda; authorities confiscated their equipment for operating without a license. Looking for income, Shakilu answered a Telegram job listing offering $1,500 a month — life-changing money in Uganda — for a salesman role. The recruiters routed him through Cambodia. He was driven eleven hours from Phnom Penh's airport to a compound and made to sign a contract he did not understand. The "salesman" job was scamming Americans.

Inside the compound, Shakilu's resistance cost him. When he failed to deliver his quota, he was made to stand facing a wall for twenty-four hours. When he again refused, he was made to hold a twenty-liter water jug at arm's length until he fainted. His leg was permanently injured. He was taken to a torture room and beaten roughly eighty times. An electric taser was applied to his handcuffed leg for fifteen minutes. When he was no longer profitable, he was sold to a second compound for thirty-six hundred dollars, which the new operators told him he would have to work off.

Shakilu reached out to me on WhatsApp in summer 2025 with his exact GPS coordinates and confirmation that his compound was actively scamming Americans at that moment. In August 2025, his messages stopped. For four months I believed he was dead. In January 2026, he reached me again. I traveled to Cambodia and met him in person where he was waiting, with more than four hundred other Ugandans, for a diplomatic waiver of overstay penalties the Cambodian government had agreed to grant in principle. Madame Betty Bigombe, the Ugandan ambassador in Kuala Lumpur who has already brought twenty-three Ugandans home from Burmese compounds, worked the diplomatic channel. Shakilu came home to Uganda. He is alive. He is not whole. He is home.

[Photo: Small Q in Uganda, taken by Erin West, November 2025]

Mwesezi — known to his fans as Small Q — is a Ugandan gospel artist who was trafficked into a Burmese scam compound near the Thai border. He spent five months inside, working twenty-hour days targeting Americans, pulling phone numbers from a list of a thousand per day with a quota of two hundred contacts. When he refused to scam on his first day, a Chinese boss tortured him for thirty minutes with an electric taser while a translator told him: *"Why have you refused to work? You are going to die in this place."* When Small Q organized a riot with other African workers, he was placed in what the compound called "the dark room" — hung from handcuffs on a meat hook for four days, in direct sun, without food or sleep. An Ethiopian man chained next to him asked for one chance to call his mother before he died. The guards beat him to death in front of Small Q. A guard then showed Small Q videos of bodies he had killed in Burma's wars and told him: *"It is nothing new to us."*

Small Q escaped by stealing an iPhone SE from a Chinese boss's office, logging into the compound's own Wi-Fi, and messaging his brother in Uganda with his location. His brother went public. Madame Betty Bigombe negotiated the release of twenty-three Ugandans. Since returning home, Small Q has used his music and his activism to raise awareness of human trafficking and scam compounds. He is now releasing an album titled *Back from Burma*. The first single is called *Dark Room*.

I share Shakilu's and Small Q's stories because the Committee's report is right that this is a polycrime ecosystem. But Shakilu and Small Q are not abstractions. They were forced to defraud Americans under torture. The American grandfather who lost ninety percent of his retirement and the Ugandan gospel artist who lost five months of his life were victims of the same enemy — sometimes through the same keystroke. The American defrauded in his living room and the Ugandan tortured in a compound four thousand miles away are on the same side of this fight.

V. THE CCP CONNECTION — WHAT I CAN SPEAK TO

I want to be honest with this Committee about where my expertise ends. The geopolitical analysis of CCP strategy is not my domain. It is yours. The Committee's report has done that work carefully, and the framework it adopts — passive tolerance, instrumental enablement, and strategic exploitation — is the right one. I endorse it without qualification. I will leave the deeper analysis of Beijing's intent to the Committee and to the scholars cited in its report.

What I can speak to is what I have seen.

I have seen the patronage networks that protect scam compounds inside Cambodia. I have stood outside Prince buildings in Phnom Penh, part of the Prince Holding Group conglomerate run by Chen Zhi. On my February 2025 trip, when I tried to film the building, I was surrounded by eight men — some armed, some wearing Cambodian police uniforms — who demanded I delete the video I had taken. That is what state protection looks like in real time. It is not theoretical. It is not deniable. It is a forced-labor scam headquarters being physically defended by the uniformed apparatus of the Cambodian state.

The United States and the United Kingdom have since identified, indicted, and sanctioned Chen Zhi and his network. Chen operated openly in Cambodia for a decade. The U.S. and U.K. unsealed the largest forfeiture in history against him in October 2025 — approximately fifteen billion dollars in Bitcoin. Chinese authorities arrested him in January 2026, only after U.S. action made him diplomatically expensive. As long as he externalized harm onto Americans, he was tolerated. The moment he became a liability to Beijing, he was extracted. That sequencing is not analysis. It is timeline.

And I have seen Dara Sakor. I drove out to Dara Sakor International Airport on my February 2025 trip. It sits on the Cambodian coast on a 99-year Chinese lease, with a 3,200-meter runway capable of handling military aircraft, in a part of the country with no commercial reason to need an airport that size. Thirty-eight miles away sits Ream Naval Base, where Chinese warships are now permanently docked. The Department of Defense and this Committee's report have both flagged what those two facilities make possible for the Chinese military on the Gulf of Thailand.

[Photo: Dara Sakor runway, taken by Erin West, February 2025]

The same Cambodian patronage networks that protect the scam compounds Americans are losing their savings to are the patronage networks that approved those leases. They are not separate phenomena. They are the same regime. The wealth Americans are losing, household by household, is reinforcing the political economy in Phnom Penh that is providing strategic access to the Chinese military on America's Indo-Pacific flank.

I do not say this to ascribe intent. I say it because it is observable. American household wealth is unintentionally underwriting hostile infrastructure. That is not consumer fraud. That is national security.

VI. WHAT CONGRESS MUST DO NOW

This Committee's report ends with seven policy recommendations. I endorse all seven. I will not relitigate them here. I will underscore the recommendations that matter most operationally, and add the asks I have been pressing for, in some cases, four years.

1. Pass H.R. 5490 and harmonize with the Cornyn-Shaheen SCAM Act (S. 2950). Together, these bills provide the clearest legislative foundation we have for treating scam compounds as the strategic threat the Committee has now formally named them. Pass H.R. 5490. Harmonize. Do not let this become the bill where bipartisan momentum dies in conference.

2. Demand accountability on the March 6, 2026 Executive Order. The Executive Order requires a comprehensive interagency action plan within 120 days. That deadline falls in early June. Congress should require that plan be delivered to the relevant committees, not just to the Executive Office. Demand a public briefing identifying the specific TCOs, the specific compounds, and the specific diplomatic consequences imposed or planned. An action plan that sits in a binder is not action.

3. Fund what the Executive Order directs but cannot pay for. An authorization without an appropriation is not a strategy. The operational cell at the National Coordination Center, the prosecutorial capacity at DOJ, and the technical assistance to state, local, tribal, and territorial law enforcement that the Executive Order calls for require dedicated, line-item funding. Directing law enforcement to fight a $4.4 trillion global criminal enterprise without funding the fight is not a national strategy.

4. Appoint a Scam Czar and stand up sustained interagency coordination. The threat cuts across DOJ, Treasury, State, DHS, FBI, FinCEN, the intelligence community, and U.S. embassies. No single agency holds the full map. Without a single accountable coordinator with the authority to convene the whole-of-government, we will continue to lose the war we are losing.

5. Build a single national victim reporting portal. Right now, victims navigate IC3, the FTC, CISA, FinCEN, and a dozen others, with no acknowledgment and no coordination. Mandate one portal, with one front door, that ingests all relevant data and routes cases automatically. We cannot size a response to a crisis we cannot accurately measure.

6. Fund state and local law enforcement and place specialized analysts at fusion centers and state high-tech task forces. When a victim like Chris calls his local police department, he should not be told they cannot help. State and local police are the first call every time. They need cryptocurrency tracing capacity and the bandwidth to triage cases in the moments when recovery is still possible. The Crypto Coalition that grew from 85 members in October 2022 to more than 2,000 today demonstrates the appetite is there. What is missing is federal investment.

7. Pass slow-the-money legislation and regulate Bitcoin ATMs. Speed is the enemy of recovery. By the time a victim realizes they have been scammed, the funds have moved at speeds that outstrip any law enforcement response. Congress should create statutory friction on high-risk transactions — wire transfers, crypto on-ramps, stablecoin conversions to high-risk addresses — and statutory tools to freeze, seize, and return funds before they vanish. Mary fed twenty-four separate cash deposits of up to $15,000 each into Wisconsin gas-station kiosks, on instructions from a criminal in West Africa, with no friction at any point in the chain. Wisconsin has now followed Louisiana's lead. Congress should follow theirs.

8. Sanction the protectors, not just the perpetrators. Apply Magnitsky aggressively and visibly. Sanction the foreign officials, business elites, militia leaders, and financial facilitators who provide political insulation to scam compounds. Apply visa restrictions to their immediate family members. Make the price of protection higher than the rents the protectors collect. The next round of designations should make clear that U.S. tolerance for protected criminality is over.

9. Ground all diplomatic engagement in verified ground truth, not Phnom Penh press releases. I have personally documented the gap between the public narrative of a "crackdown" and the reality of a relocating, expanding industry. Congress should require independent verification — by U.S. embassies, by intelligence assets, by partner-supported civil society — before diplomatic concessions or normalization are offered. Performative crackdowns must not be rewarded.

10. Engage the private sector as a national security partner. Meta repeatedly told Chris the scammer's profile did not violate community standards. Match Group has biometric tools that could detect the impersonator profile used to scam Mary. These are corporate governance failures with national security consequences. Congress should require structured public-private information sharing, typology development, rapid reporting channels, and risk-based guardrails at every chokepoint where the criminal model has industrialized victim acquisition.

11. Coordinate with allies, and cooperate with the PRC tactically — never strategically. Pressure in Cambodia and Myanmar is already pushing operators into the Pacific Islands, the Gulf, Africa, and Latin America. Sustained alignment globally is the only way to prevent another decade of whack-a-mole. Welcome PRC cooperation where it produces verifiable gains. Do not mistake tactical cooperation for alignment of incentives. Beijing acts decisively when its citizens or reputation are at stake. It tolerates harm to ours.

VII. CONCLUSION

I have been saying for four years that we are at crisis level and we must act. Four years.

In the twenty months since I last testified before Congress in person — in September 2024 — tens of billions of dollars more have been stolen from American households. Tens of thousands more people have been trafficked into compounds to do the stealing. The compound infrastructure has not been dismantled. It is relocating into terrain harder to investigate, harder to raid, and harder to disrupt. The crime has expanded from financial fraud into the sexual exploitation of American children. The proceeds are funding patronage networks that are providing strategic access to the Chinese military on the Cambodian coast.

This Committee has now done what no previous body has done. You have named the threat. You have framed it correctly. You have placed the weight of this institution behind a careful, defensible diagnosis. The American public has needed Congress to say plainly what is happening, and Congress has now said it.

The question that remains is whether the diagnosis becomes a response.

Chris was told his loss was too small to matter. Cristy was told there was nothing federal law enforcement could do. Don and Mary built investigations the federal response should have built and are still waiting for the federal response to use what they found. Shakilu escaped a Cambodian compound and is rebuilding his life in Uganda. Small Q watched a man die and stole an iPhone to save twenty-three other people. Three fathers' families learned why they died only by going through their digital lives after the fact. Every constituent in every district at this dais is being targeted today, right now, while we sit in this room.

They cannot afford another year. Neither can we.

Thank you for the opportunity to testify. I welcome your questions.

Respectfully submitted,

Erin West

Founder and Chief Executive Officer, Operation Shamrock

www.operationshamrock.org