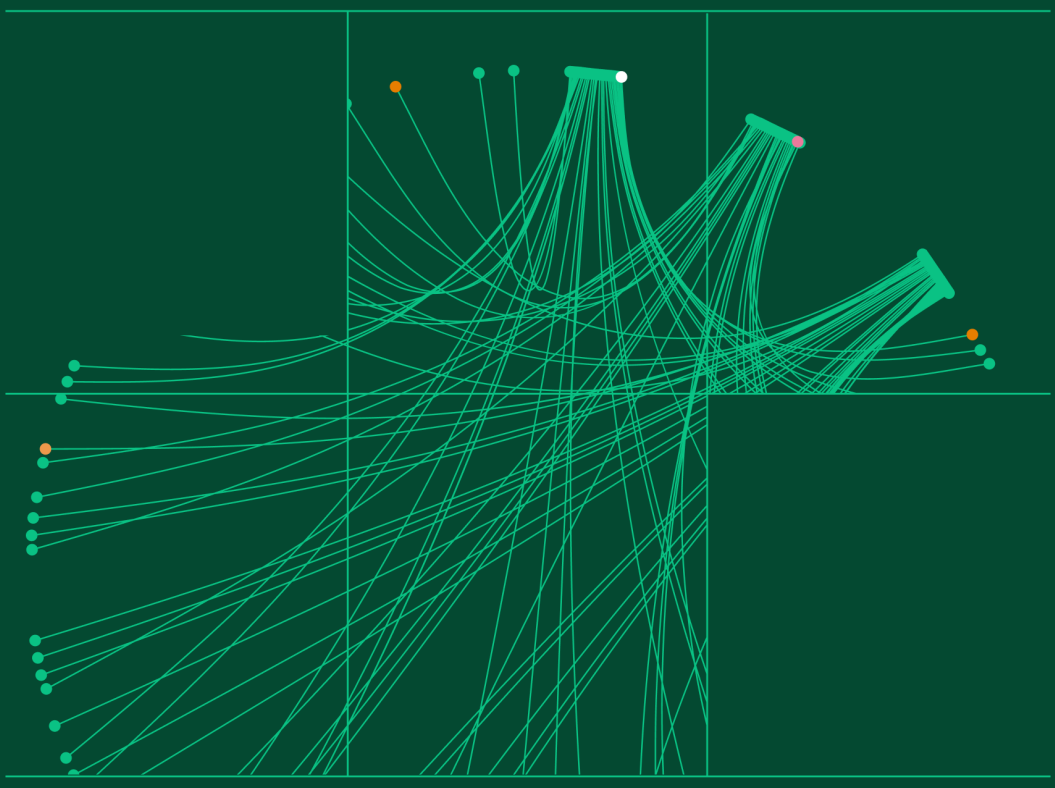
WHITEPAPER

Ending the Scamdemic: The Case for a Global Scam Action Task Force (SATF)

Sardine | SHAMROCK



ENDING THE SCAMDEMIC

The Case for a Global Scam Action Task Force (SATF)

Authors:

Sardine and Operation Shamrock.

Sardine Collection

Table of Contents

Introduction: The Invisible War That's Already Here

Mwesezi tried to escape once. They hung him by his arms for three days.

His crime? Refusing to destroy strangers' lives from a computer in Myanmar. Under threat of violence, he and hundreds just like him are forced to spend 16 hours a day side-by-side in front of screens, pretending to fall in love with lonely Americans. Miss your quota of stolen hearts and money? Get beaten. Try to leave? Get tortured.

This is the hidden half of every romance scam: the person forced to type 'I love you' while a gun points at their head to steal the life savings of victims in the G20.

Criminals use forced labor to run a global network of scams. Every pig butchering scam

has two victims: The one who sends their life savings. And the one forced to take it. This is industrial-scale human trafficking. Criminals have built entire cities, walled compounds with guards, weapons, and high-rise towers dedicated to scamming the world.

Transnational criminal organizations have established elaborate "scam cities", industrializing human trafficking and financial fraud. Criminal revenues from online scams are growing 40% every year[1]. Chainalysis tracked a 210% surge in scam-related crypto deposits from 2023 to 2024. If that pace continues, what was $100 billion in 2023 will reach $400 billion by 2027.

The world's response is fragmented. Coordination is weak, legal frameworks are unclear, and criminals exploit every delay. Yet there are pockets of good practice worth scaling:

- Operation Shamrock[2] has shown that law enforcement can rapidly learn new skills and become effective against transnational crime.
- Digital banks are implementing new AI-

powered detection and user experience flows to add friction and break the scammers' spells.

- Cross-industry data sharing utilities like Sonar[3] are appearing that can improve our global coordination.

While these early victories prove what's possible, these remain a drop in the ocean compared to the scale of response required to end the Scamdemic.

The Scale of the Numbers Demands Action

$64B stolen annually

By regional scam syndicates worldwide[4]

250,000+ people

Currently enslaved across compounds[5]

120,000 trapped

In Myanmar, and 100,000 trapped in Cambodia[6]

10+ countries

with scam compounds and expanding[7]

This paper makes the case for the Scam Action Task Force (SATF), a permanent, global body with the power to dismantle scam networks, free the trafficked, and protect citizens' savings. Modeled after the Financial Action Task Force (FATF) that reshaped global money laundering enforcement, SATF would bring binding standards, real consequences, and coordinated action to match the scale of this Scamdemic.

To match the scale of this threat, SATF's mandate must drive a coordinated global counter-offensive through 10 urgent actions:

1. Declare a global emergency on scams
2. Establish SATF with enforcement power
3. Mandate proven scam detection technologies
4. Build real-time intelligence sharing networks
5. Arm law enforcement with tools to catch digital crime

6. Destroy criminal infrastructure through international cooperation
7. Standardize the recovery of funds for victims globally
8. Protect the public with awareness campaigns and simple, direct reporting tools
9. Hold industries and governments accountable for scam detection
10. Fund the Scam Action Task Force with project goals and a clear mandate

At 40% annual growth, today's $75 billion becomes $10 trillion by 2030. For a fraction of that, we can fight back.

01

The Infrastructure of Modern Crime

The Criminal Cities

Cambodia has become the world's first scam economy. Every level of society has been corrupted by scam money, creating a political economy where fighting crime means destroying livelihoods. As transnational organized crime expert Jacob Sims observed in his recent paper[8], this represents "the first time in modern history that a nation has industrialized human trafficking as a pillar of economic development."

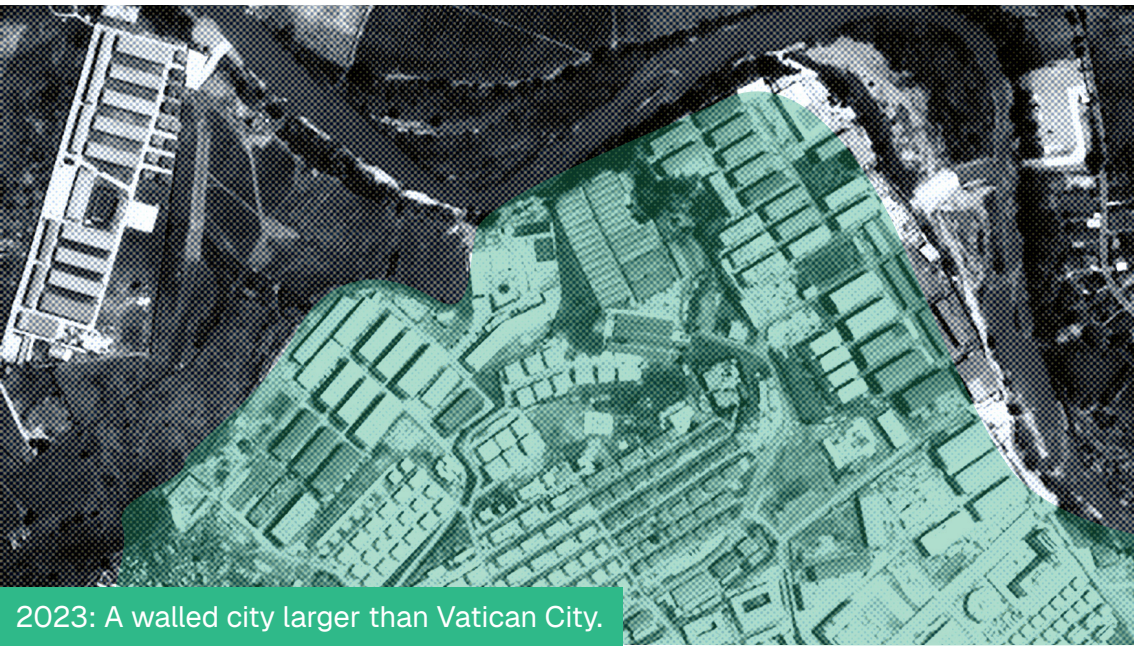
In March 2025, former prosecutor Erin West travelled to Cambodia. She had recently left her 26-year-career as a prosecutor to found a non-profit called Operation Shamrock, dedicated to disrupting transnational organized crime. What she saw was staggering. High-rise compounds everywhere - residential towers surrounded by perimeter walls and guarded entry points staffed with armed personnel carrying machine guns. These facilities function as closed systems where trafficked individuals work under coercion.

Locals call what happens inside “online” - a euphemism for industrial-scale fraud. Despite efforts to sanitize the public image, digital fraud has become a significant industry in Cambodia. Construction cranes work around the clock. Massive dormitory-style buildings rise in plain view. Aggressive growth was visible at multiple locations in the country.

Myanmar’s KK Park: From Farmland to Scam City. Growth is also the standard on the Myanmar-Thailand border, near Myawaddy. KK Park was one of the earliest compounds built exclusively for scam operations.

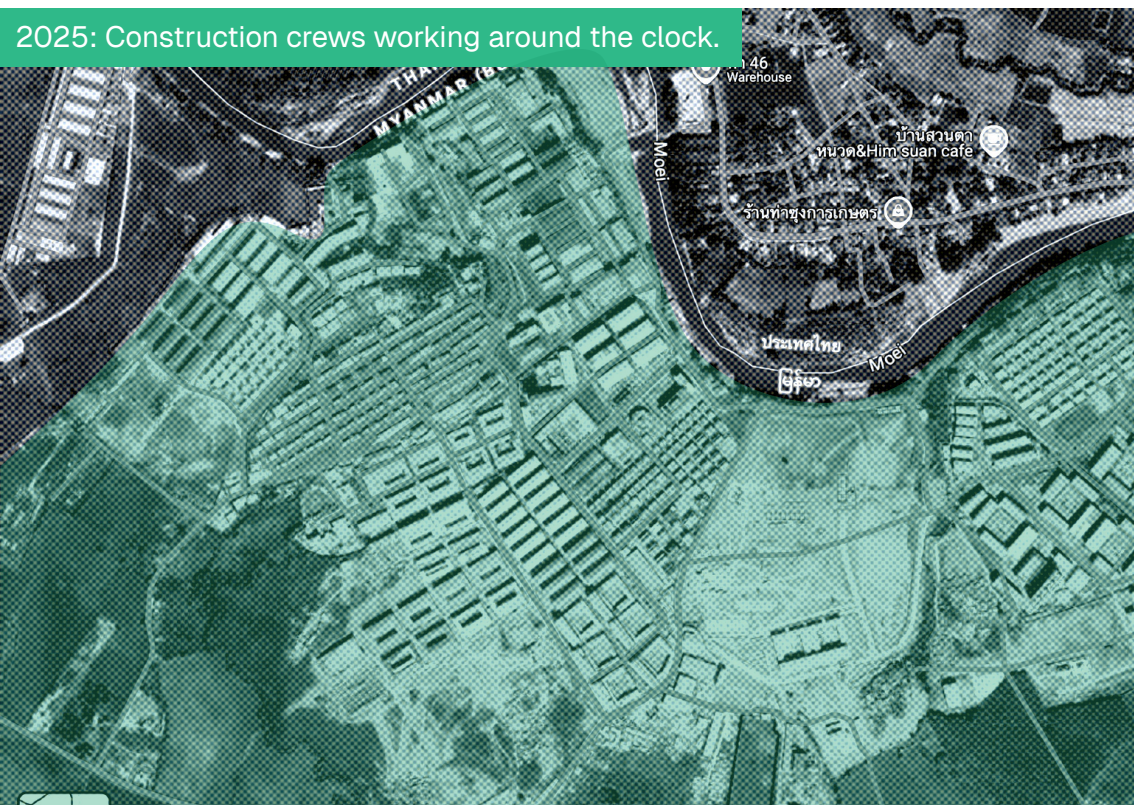
Here’s what Google Earth shows:

2020: Empty farmland on the Myanmar side of the river.

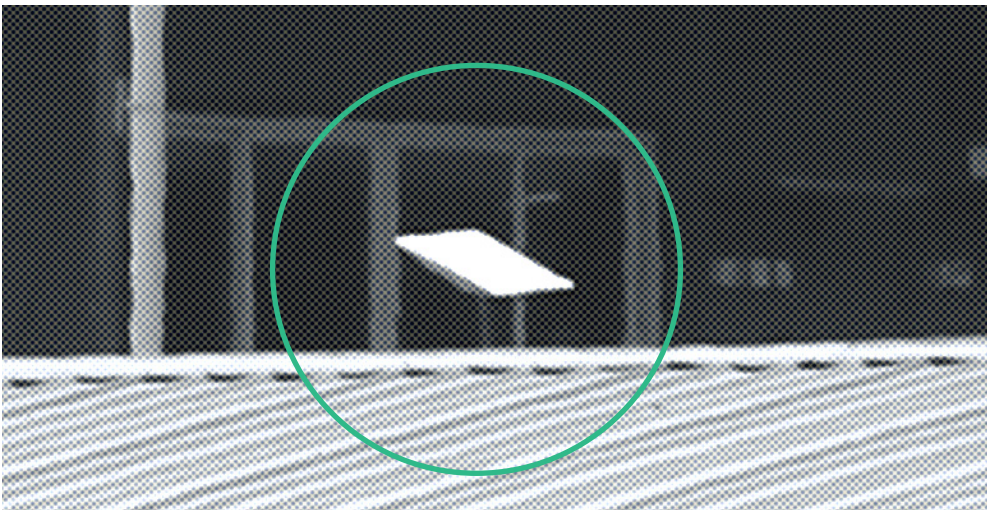


2023: A walled city larger than Vatican City.

2025: Construction crews working around the clock.



The cement trucks drive across from Thailand every morning. The guards carry AK-47s. The Starlink dishes throughout the park beam stolen crypto out of government reach.



Reference: Closer view a Starlink receiver at KK Park, credit Cezary Podkul

Key infrastructure elements documented:

- Perimeter walls with guard towers
- Dormitory-style housing for an estimated 10,000 individuals
- Starlink satellite Internet installations providing connectivity
- Regular cement truck deliveries from Thailand indicating ongoing construction

Construction continues: a further check of Google Earth at the time of this writing in July 2025 reveals that the dirt patch in the center of the photo now houses operational multi-story buildings.

Reference: Cement trucks take raw materials from the factory in Thailand across the river to KK Park. (Credit Erin West)

The Philippines: A Window Into Operations

The Philippines recent raids, deportations, and interagency investigations allowed Erin West unprecedented access to examine raided scam centers. What she found confirmed the industrial scale: professional setups rivaling

legitimate call centers, training materials for psychological manipulation, and infrastructure for processing millions in stolen funds.

The Philippine government's crackdown shows what's possible when nations take this threat seriously.

Global Spread: Find Success and Repeat

West's March 2023 trip to Dubai revealed how easily these operations transplant. Photos show Chinese-run scam centers operating in Dubai's outskirts - the same model, different location. Authorities have since raided similar

compounds in Peru, Isle of Man, Pakistan and Sri Lanka.

The model is proven and portable:

> Trafficked labor + Internet access + weak governance = profit center.

The Business of Industrialized Crime

B

Scams are a highly lucrative industry, and the Growth Trajectory is at an Epidemic Level

- Criminal revenues are **growing 40% year-over-year**[9]
- Crypto deposits to scam address **surged 210%**[10] from 2023 to 2024
- **Victims lost $4.6 billion**[11] to cryptocurrency investment scams in 2023
- By 2024, investment fraud alone hit **$5.8 billion**[12]
- In 2024, The United States Institute of Peace said that by conservative estimates, global financial losses to scams have reached **$64 billion annually**[13]

For deeply personal scams like pig butchering, where victims feel profound shame, the

reporting rate drops even lower. The real scale could be 15 to 20 times larger than official figures, suggesting we are looking at a trillion-dollar criminal economy operating in plain sight.

At 40% annual growth, criminal revenues double every two years. What was $100 billion in 2023 becomes $400 billion by 2027. Victim counts are growing even faster than revenue, and geographic expansion is accelerating.

AI Deepfakes are now Near Perfect for Scamming

Recent conversations with Operation Shamrock victims reveal just how devastating this technology has become.

> One victim, a well-educated man, was absolutely convinced he'd been talking to the former Miss Universe of Malaysia. He reverse-image-searched her photos and found her profile online. But what convinced him beyond doubt were their video calls - she had the exact same mole as in her pictures, the same mannerisms, the same voice he'd

> imagined. When the Operation Shamrock team tried to explain deepfake technology, he refused to believe it. The technology was that convincing.

Scammers now use AI-generated audio and video to impersonate anyone - romantic partners, financial advisors, even law enforcement. The deepfakes are so sophisticated they fool facial recognition software. Voice cloning creates pitch-perfect audio in any language or accent.

How Cybercrime Became Big Business

Modern scam operations look and function just like major tech companies. They've created "Scam-as-a-Service" platforms where experienced fraudsters sell ready-made templates, scripts, and automated tools. Successful scam methods get packaged and sold like franchise opportunities - think McDonald's, but for fraud. Telegram channels and dark web sites work like criminal app stores, selling everything you would need to open your own scamming business.

What Scammers Can Buy Online

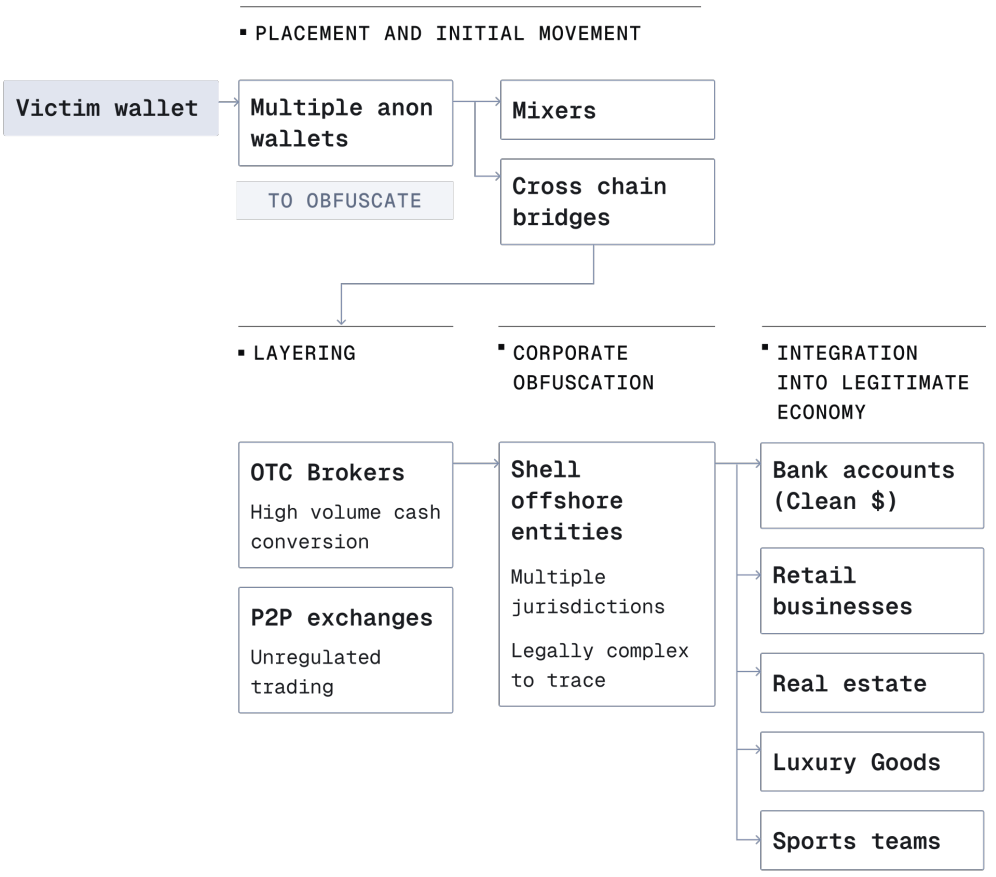
- **Fake investment websites** - Ready-made trading platforms that look identical to legitimate cryptocurrency exchanges
- **AI face-swapping software** - Technology to create deepfake videos for video calls with victims (around $200)
- **Stolen personal data** - Contact lists, phone numbers, and personal information for targeting victims
- **Money laundering services** - Converting victim payments into cash, stable cryptocurrencies, or Chinese payment app credits
- **Social media accounts** - Fake profiles with established histories for building trust with targets
- **Torture and control devices** - Electric batons and shock-enabled tracking devices used to control trafficked workers

- **Training materials** - Scripts and psychological manipulation techniques for romance scams
- **Cryptocurrency conversion** - Services to quickly move and hide stolen digital assets

These groups have actual HR departments that post fake job listings on legitimate job sites. They run training programs where kidnapped workers learn psychological manipulation techniques. They use performance management systems with daily targets, quality ratings, and bonuses for top performers. They even have research and development teams constantly testing new technologies and scam typologies and improving their methods based on data.

Reference: Example of job advertisement used by scammers

Obfuscation at Scale: How Dirty Money Disappears



Victim funds travel through an intentionally tangled web: bounced between crypto wallets, funneled through shell companies, converted by underground brokers, transformed into

stablecoins, Chinese payment credits, or hard cash and ultimately cycled into legitimate business. Services offered through platforms like Huione Guarantee make this easy, with criminals able to purchase end-to-end laundering packages. The platform processed an estimated **$11 billion in tainted funds** before it was shuttered in May 2025. New platforms have already risen to take its place.

Monica - The Victim You Know

Mwesezi's Story - The Victim You Don't Know

The Truth Nobody Wants to Hear

02

The Human Cost: Two Victims, One Crime

Monica - The Victim You Know

A

Monica was 40, drowning in student loans from getting her PhD. Like millions of people, she tried online dating. That's where she met "Ethan."

He was perfect. Successful investor, great listener, genuinely interested in her triathlon training. They texted for hours every day. When Monica joked about being happy with her Garmin watch while he shopped for Rolexes, Ethan offered to teach her investing. He could help her get out of debt.

It worked at first. She doubled her money. So she pulled from her retirement account. Then came the fees. The taxes. Monica took out loans at 38% interest to cover them. By the time her family realized what was happening, everything was gone.

Mwesezi's Story - The Victim You Don't Know

B

Mwesezi was 23, making less than $100 a month at a Kampala Internet café. When a fellow Ugandan offered him an IT job in Bangkok for $1,000 monthly, he jumped at the chance.

But there was no IT job. After a 24-hour journey from Bangkok airport, Mwesezi found himself in a walled compound in Myanmar, guarded by men with assault rifles. Inside, hundreds of people sat at computers. His real job: pretend to be someone else online and convince people to send money.

Try to escape? Mwesezi tried once. They caught him and hung him by his arms for three days.

For months, he typed love messages and investment advice to strangers, hating himself

for destroying their lives but knowing that refusing meant risking his own. When he finally stole a phone and contacted a Ugandan official on Facebook, it took weeks of diplomatic pressure to get him out.

He spent every day destroying innocent people's lives to save his own.

Mwesezi immediately after his rescue. He stands on the Thai side of the Moei river with the compound and Myanmar behind him.

The Truth Nobody Wants to Hear

C

These two stories expose the systemic failures that must be fixed if we ever want to stand a chance in this fight. Monica lost her life savings to someone like Mwesezi - not a criminal mastermind, but a trafficking victim forced to scam at gunpoint. This is the sick genius of modern organized crime: They enslave people and force them to do the stealing.

Only global cooperation can truly turn the tide on these networks. That’s why we need a Global Scam Action Task Force to coordinate the multinational response needed to shut down these operations faster than criminals can build them.

Jurisdictional Borders vs Borderless Crime

Outdated Legal Frameworks Make The Issue Worse

Industry Sectors Don’t Collaborate to Solve the Global Issue

The Gaps We Must Close

03

Jurisdictional Borders vs Borderless Crime

A

By the time Monica's family realized what happened and looked for assistance, they faced a crushing reality: no one would help them.

- The local police said they couldn't investigate international crypto fraud.
- The FBI's IC3 took her report but warned that international cases rarely see resolution.
- The dating app claimed no responsibility.
- The crypto exchanges pointed to their terms of service.

Meanwhile, her money had crossed through at least six jurisdictions, each with different laws, different enforcement capabilities, and zero real-time cooperation.

Six jurisdictions. Six different legal systems. Zero real-time cooperation.

> The Federal Trade Commission estimates only 6% of fraud victims come forward. For romance scams involving intimate conversations and devastating financial loss, it's likely even lower. As one victim told Operation Shamrock, "I was too ashamed to tell anyone. I thought I was smarter than this."

Consider Mwesezi's perspective from inside the compound.

- He knew he would get no help in Myanmar - the compound operators were protected by armed militia groups.
- Ugandan authorities had no jurisdiction in Myanmar.
- The international community seemed unaware these compounds even existed.

Outdated Legal Frameworks Make The Issue Worse

B

Law enforcement lacks the tools, training and coordination to be effective against a criminal global enterprise moving money in cryptocurrency. When law enforcement first started seeing these cases in 2021, most investigators had never used blockchain analysis tools. They didn't understand how cryptocurrency worked, much less how to trace it."

- Prosecutors didn't know how to present cryptocurrency evidence to judges who'd never heard of blockchain.
- Courts lacked precedents for international crypto asset seizures.
- Even when investigators identified stolen funds, the legal framework for recovery hadn't caught up to the technology.

- There's no single database to track all reports across jurisdictional lines.
- And no single reporting hub for victims like Monica or Mwesezi to report what they've been exposed to.

The laws governing financial crime were written for a different era.

- The Bank Secrecy Act dates to 1970. The Wire Fraud statute to 1952.
- Human trafficking laws assume physical movement for traditional exploitation, not digital fraud.
- International agreements on law enforcement cooperation assume physical borders matter and that crime happens slowly enough for formal diplomatic requests.

By the time a Mutual Legal Assistance Treaty request makes its way through diplomatic channels - often taking 6-12 months - the criminal networks have evolved their tactics, moved their operations, and trafficked in new victims.

Even successful prosecutions often fail to help victims. Criminal forfeiture proceedings can take years. Civil recovery requires victims to hire lawyers they can't afford after losing everything. International asset recovery involves navigating legal systems in countries that may be complicit in the crimes. And for trafficking victims like Mwesezi? They're often treated as criminals themselves, deported or prosecuted for the fraud they were forced to commit.

Industry Sectors Don’t Collaborate to Solve the Global Issue

C

There’s no clear legal framework for cross sector collaboration.

- **The banks operate under the Bank Secrecy Act and Anti-Money Laundering rules** that were written for drug traffickers moving cash, not tech-savvy criminals moving cryptocurrency.
- **Telecom companies hide behind the Telephone Consumer Protection Act,** focused on robocalls and spam, while scammers use sophisticated VoIP systems to spoof legitimate numbers.
- **Social media platforms and dating apps (where most victims first meet scammers) point to their Terms of Service and claim they’re not responsible for user behavior.**

While they may remove fake accounts after they're reported, enforcement is slow and inconsistent. Trust and Safety teams are often under-resourced, siloed, and rarely coordinate across companies. There is no industry-wide system for sharing intelligence about known scam networks, even when the same fake personas appear on multiple platforms.

- **Satellite Internet provides high-speed Internet to remote locations** including scam compounds in Myanmar and Cambodia. While it serves legitimate purposes, it has become the connectivity provider of choice for criminal operations.

Social media algorithms, designed to maximize engagement, actively promote fake profiles that show signs of high interaction. A scammer who gets victims to message frequently is rewarded with greater reach.

Success stories prove this isn't inevitable. When we enable real-time coordination, share intelligence across borders, understand the

dual-victim nature of these crimes, and give law enforcement proper tools, we win. The technology exists. The legal frameworks can be updated. The cooperation mechanisms can be built.

A. Effective Data Signals, UX Patterns & Reporting Approach

B. Government Actions That Work

C. Industry & Law Enforcement Coordination That Works

Early Victories Prove SATF Would Work

Pockets of industry and government have shown that direct intervention can turn the tide of this war. From Singapore's lightning-fast recovery protocols to Operation Shamrock's grassroots law enforcement revolution, we have proof that coordinated action defeats criminal networks.

Effective Data Signals, UX Patterns & Reporting Approach

A

Modern real-time data signals can detect scams before they happen: Typing patterns, calls in session, and remote screen sharing activity can be high risk early warning signals of a scam about to happen.

- By using these signals, clients of Sardine report 95% reduction in scam losses within months of implementation.
- One major fintech saw scam losses drop 94% in the first month using platforms that combine behavioral biometrics, device intelligence, and AI-powered anomaly detection.

When institutions detect red flags, they intervene with protective friction: These

interventions work because they break the spell, disrupting the psychological grip scammers hold over victims.

- Clear warning messages that explain specific risks
- Mandatory cooling-off periods for high-risk transfers
- Videos and scam awareness education for suspected victims
- Transaction verification through secure, independent channels, such as an owned mobile app, no direct calls outside of that channel

The UK's Banking Protocol shows the power of simple coordination. When staff suspect a customer is being scammed, they immediately alert law enforcement. The results:

- 75% arrest rate for suspects still at the scene
- Over £258.2 million prevented since 2016
- 1,202 arrests

Government Actions That Work

B

Singapore's Anti-Scam Centre demonstrates how rapid intervention, technology, and partnerships create a powerful defense against fraud:

- Transformed account freezing from a two-week process to <24 hours
- Co-located staff from six major banks for seamless coordination
- When a scam is detected, bank representatives can freeze accounts immediately while police trace funds and tech partners block malicious content simultaneously

This ecosystem approach has recovered over $200 million since 2019, with recovery rates as high as 40.8%.

In the Philippines, coordinated raids on scam compounds exposed their industrial scale:

professional setups rivaling legitimate call centers, detailed psychological manipulation training materials, and infrastructure for processing millions in stolen funds.

When governments act decisively, coordinate across agencies, and cooperate internationally, criminals lose their safe havens.

Industry & Law Enforcement Coordination That Works

C

The Sonar Consortium proves that real-time intelligence sharing among nonbanks and financial institutions creates an impenetrable defense network.

- Open to banks and non-banks, with 80+ stakeholders from digital assets, payments, marketplaces, and telecom
- When one detects a new scam pattern, every institution in the network benefits
- A scam that would have worked on thousands fails after the first attempt
- Enables officers to intercept funds before scammers can move them

The Operation Shamrock Crypto Coalition started with 85 participants in 2022. In just over

two years, it exploded to 2,500 active members from local, state, federal, and international agencies across all 50 U.S. states and multiple countries. It's credited with tens of millions of dollars in victim recoveries.

Members report breakthroughs weekly: frozen accounts, traced funds, victims being heard. By building an informal network that operates at Internet speed rather than bureaucratic pace, they've proven that law enforcement can match criminal agility.

05

The 10-Point Strategy to End the Scamdemic

Declare a Global Security Emergency

/1

Call this what it is: warfare. Criminal organizations steal hundreds of billions while enslaving 250,000 people. G20 nations should declare transnational scams a global security emergency to unlock the powers and resources used against terrorism or military threats.

This declaration would trigger rapid cooperation, bypass bureaucratic delays, and enable emergency funding. No more committees studying the problem while compounds expand and victims multiply. This is war, and we need to fight it with wartime urgency.

Establish the Scam Action Task Force (SATF)

/2

The Financial Action Task Force (FATF) is a global organization that sets the rules for fighting money laundering, terrorist financing, and other financial crimes.

The Scam Action Task Force would do the same for scams, serving as the permanent international body to set and enforce mandatory cross-sector rules for banks, telecoms, and platforms. It would also establish 24-hour cross-border fund recovery protocols, replacing today's system where mutual legal assistance takes months while money vanishes in minutes.

Most critically, SATF would have the power to graylist non-compliant jurisdictions. Countries that harbor scam compounds or refuse to implement standards would face the same reputational and economic consequences

as money laundering havens. When hosting scammers costs more than bribes pay, governments will act.

Deploy Proven Financial Defense Technology and UX /3

Every financial institution worldwide must implement behavioral biometrics to detect when customers are under duress or subject to a potential deepfake. AI anomaly detection should flag suspicious transactions before money moves.

- **Liveness, deepfake and mask detection** must defeat AI fakes attempting to authorize transactions.
- **Three-hour cooling-off periods** for high-risk transfers give victims time to break free from manipulation.

These technologies exist. Sardine and others have built them. They work. The only barrier is mandating their use.

Build Real-Time Intelligence Networks

/4

Criminals share intelligence instantly and globally. A new scam technique discovered in Cambodia appears in Canada within days. Our response must be equally rapid. We need secure data pipelines connecting banks, law enforcement, telcos, and platforms in real-time.

- **Consortium models like Sonar must be mandatory, not optional.** When one bank detects a scam pattern, every institution should know within milliseconds.
- **One-click reporting should be the standard.** The current maze where victims file reports with multiple agencies that never connect doesn't work. Intelligence must flow at the speed of crime, not the pace of bureaucracy.

Arm Law Enforcement for Digital Combat

/5

Every police department needs officers who understand cryptocurrency, can trace digital assets, and recognize the signs of pig butchering scams. Law enforcement can achieve remarkable results with proper tools and training:

- Create regional hubs worldwide where investigators share knowledge in real-time.
- Provide blockchain analysis tools to every jurisdiction.
- Train rapid response teams for scam compound raids, combining financial investigation skills with anti-trafficking expertise.

The goal: train 100,000 officers in digital asset investigation by 2026.

Destroy Criminal Infrastructure Faster Than They Build

/6

Scam compounds take years to build but should take hours to shut down. With real-time systems, we can dismantle criminal infrastructure at digital speed.

A fake investment platform should be offline before the first victim loses money. Spoofed numbers should blocked by telecoms instantly. Coordinated compound raids must become regular, not exceptional. Crypto wallets tied to scams should be frozen within hours.

The goal is to make running scams costlier and riskier than the profits they generate. If criminals can’t keep infrastructure up long enough to recoup investment, they’ll move on.

Mobilize and Protect the Public

/7

Shame keeps victims silent and criminals profitable. We can change that with prevention, which costs pennies compared to recovery.

- **Fund awareness campaigns** led by survivors like Monica and Mwesezi.
- **Mandate scam education** in schools, workplaces, and community centers.
- **Build community protection networks** to ensure vulnerable populations have advocates watching for signs of exploitation.
- **Launch 24/7 “Is this a scam?” services** for verifying suspicious contacts.

If we make scam protection as accessible as 911, we can help break the spell scammers cast.

Standardize Global Recovery Protocols

/8

Every country needs legal frameworks enabling instant fund freezing when scams are detected. Singapore proves 90% recovery is possible within 24 hours. This should be the global standard, not an outlier.

- **Create fast-track mutual legal assistance** for scam cases. Current treaties taking 6-12 months are useless against crimes measured in minutes.
- **Establish clear recovery paths** victims can follow without hiring expensive lawyers.
- **Standardize procedures** so a scam reported in Germany can freeze funds in Dubai.

Instant global money movement requires legal systems to match that speed to remain effective.

Hold Everyone Accountable

/9

What gets measured gets fixed. Public scorecards should rank every country on anti-scam performance: prevention rates, recovery speed, prosecution success, and compound closures. Jurisdictions enabling scammers must be named and shamed, and those taking action should be recognized.

Platform accountability must be part of the solution. Social media, telecoms, satellite Internet, and messaging services are often the channels criminals exploit. These industries have the tools and reach to make scams far harder to operate. That means:

- Proactive detection of scam profiles using existing AI capabilities.
- KYC for satellite Internet in high-risk regions

- Financial liability when platforms ignore clear patterns of criminal behavior.
- Public reporting on scam origination to create market incentives for improvement.

Financial institutions must also lead by example. Deploying proven real-time detection technologies is essential to protect customers. Independent compliance audits, along with quarterly public reporting on funds recovered, criminals prosecuted, and victims protected, would strengthen transparency and demonstrate the sector's commitment to combating scams.

Fund the Fight Like We Mean It

/10

Fighting scams requires real investment. SATF would need $10B to build infrastructure, train personnel, and coordinate a global response. That's less than two weeks of current criminal revenue against a trillion-dollar threat.

Sustainable financing can come from mandatory industry contributions based on scam volumes flowing through their systems. Banks, crypto exchanges, payment platforms, and telecoms profiting from transaction fees should help defend those transactions. Seized criminal assets should fund victim recovery, creating a virtuous cycle where crime finances its own defeat.

Every dollar spent on prevention saves hundreds in losses, prevents thousands of victims, and protects millions of potential targets.

The Strategy Is Here - Execution is Next

Ten concrete steps. Each proven possible by existing successes. Together, they form a comprehensive battle plan that matches criminal sophistication with coordinated defense. We don't need new technology or novel legal theories. We need the courage to implement what we know works.

This strategy ends the Scamdemic. The only question is whether we'll implement it before the cost becomes unbearable.

CONCLUSION

SATF - The Only Solution That Matches the Threat

SATF would do what no current body can: coordinate instant response across borders, mandate proven technologies globally, and gray-list nations that harbor criminal operations.

Within 24 months of SATF's establishment, we would see:

- Scam attempts drop as prevention tools become universal
- Recovery rates rising through 24-hour cross-border protocols
- Countries choose compliance over criminal money as gray-listing takes hold

The Philippines showed what national action can achieve. Singapore proves rapid recovery is possible. Operation Shamrock shows coordination works. SATF would make these isolated wins the global standard.

The Cost of Rejecting SATF

Without SATF, we're choosing catastrophe. At 40% annual growth, today's $75 billion in scam revenues becomes $10 trillion by 2030. The 250,000 people currently enslaved will swell past 1 million. Every delay means more lives destroyed, more families bankrupted.

Why SATF, Why Now

This is our FATF moment. When money laundering threatened the global financial system, the world created the Financial Action Task Force with binding standards and real consequences. FATF transformed how nations combat financial crime. SATF would do the same for scams.

The Call to Action: Be The People Who Stopped This

To G20 Leaders: You have the power to create SATF at your next summit. The proposal is ready. The framework is proven. The cost of delay is measured in destroyed lives. Make SATF your legacy, the moment democracies fought back against digital slavery.

To Financial Ministers: Champion SATF in every international forum. You've seen what FATF achieved for money laundering. SATF would do the same for the trillion-dollar scam economy. Push for its creation with the urgency this crisis demands.

To Financial Institutions: Support SATF's creation vocally and prepare for its standards. You know voluntary measures have failed. SATF would create the level playing field where

security becomes a competitive advantage, not a costly burden.

To Law Enforcement: Make SATF your rallying cry. You're fighting 21st-century crime with 20th-century tools. SATF would give you the authority, resources, and coordination to win. Demand it from your leadership.

To Technology Platforms: You are best placed to help scale SATF and help shape standards now.

Final Thought: SATF Is Not Optional

Every day without SATF, another thousand Monicas lose everything. Another hundred Mwesezis are trafficked. Criminal revenues grow by millions. The question isn't whether we need SATF. It's whether we'll create it before the cost becomes unbearable.

Monica deserves justice. Mwesezi deserves freedom. Millions of future victims deserve protection. They’re not asking for charity, they’re asking for someone to fight for them.

The choice is ours. The time is now. SATF how we fight back.

References

[1] **Chainalysis**. “Pig Butchering Scam Revenue Grows YoY.” February 29, 2024. Accessed August 19, 2025. Chainalysis. https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/

[2] **Operation Shamrock**. “Operation Shamrock.” Accessed August 19, 2025. https://operationshamrock.org/

[3] **Sonar.** “Sonar.” Accessed August 19, 2025. https://www.joinsonar.com/

[4] **United States Institute of Peace. Transnational Crime in Southeast Asia.** May 2024. Accessed August 19, 2025. https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

[5] **Office of the High Commissioner for Human Rights.** “Online Scam Operations Trafficking Tens of Thousands in Southeast Asia, Warns

UN." August 29, 2023. Accessed August 19, 2025. United Nations. https://www.ohchr.org/en/press-releases/2023/08/online-scam-operations-trafficking-tens-thousands-southeast-asia-warns-un

[6] **Office of the High Commissioner for Human Rights.** "Hundreds of Thousands Trafficked to Work for Online Scammers in Southeast Asia, Says UN Report." August 29, 2023. Accessed August 19, 2025. United Nations. https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report

[7] **Legal News Feed.** "UN Alerts on Escalating Human Trafficking Crisis in Southeast Asia's Scam Compounds: A Call for Urgent Global Action." May 21, 2025. Accessed August 19, 2025. Legal News Feed. https://legalnewsfeed.com/2025/05/21/un-alerts-on-escalating-human-trafficking-crisis-in-southeast-asias-scam-compounds-a-call-for-urgent-global-action/

[8] **United States Institute of Peace.** Policies and Patterns. May 16, 2025. Accessed August 19, 2025. https://cdn.prod.website-files.com/662f-5d242a3e7860ebcfde4f/68264cff356caba111f-2db1e_Policies%20and%20Patterns_16052025.pdf

[9] **Chainalysis.** "Pig Butchering Scam Revenue Grows YoY." February 29, 2024. Accessed August 19, 2025. Chainalysis. https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/

[10] **Chainalysis.** "Pig Butchering Scam Revenue Grows YoY." February 29, 2024. Accessed August 19, 2025. Chainalysis. https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/

[11] **Federal Bureau of Investigation.** 2023 Internet Crime Report. 2024. Accessed August 19, 2025. Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

[12] **Federal Bureau of Investigation.** 2024 Internet Crime Report. 2025. Accessed August 19, 2025. Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[13] **United States Institute of Peace.** "Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security." May 7, 2024. Accessed August 19, 2025. https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security