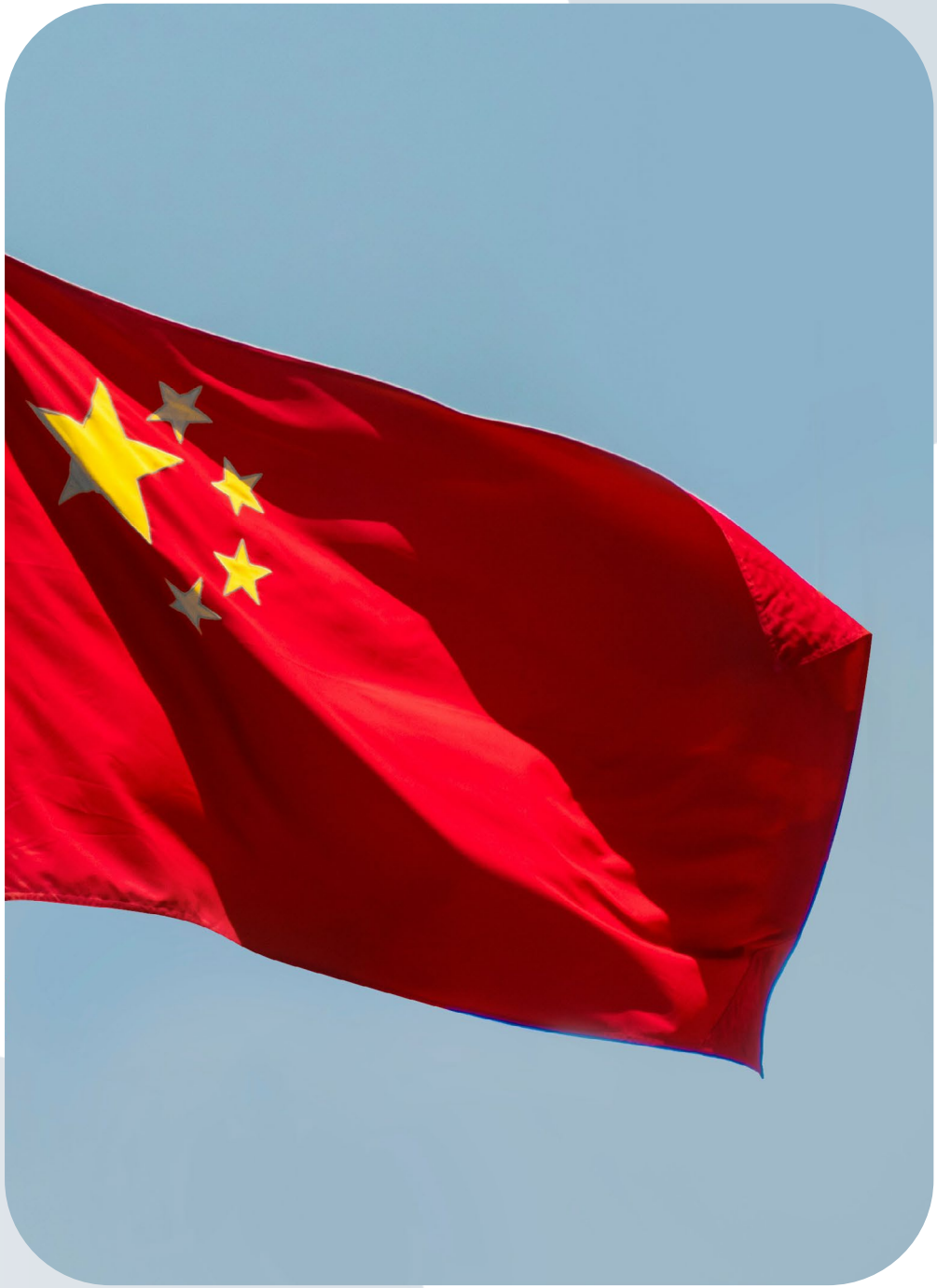
THEMIS

China

COUNTRY RISK BRIEFING - 2025



WWW.WEARETHEMIS.COM

Country Overview

Location:
East Asia, bordered by 14 countries including Russia, India, and North Korea

Capital:
Beijing

Currency:
Chinese Yuan (CNY/RMB)

Population:
Approximately 1.41 billion (United Nations, 2024)

GDP:
$18.5 trillion nominal GDP (World Bank, 2024)

Major Economic Sectors:
Oil and gas, petrochemicals, financial services, ICT, construction

Natural Resources:
Coal, iron ore, petroleum, natural gas, mercury, tin, tungsten, antimony, manganese, molybdenum, vanadium, magnetite, aluminium, lead, zinc, uranium

Government:
One-party, nominally socialist republic led by the Chinese Communist Party

Economy & Politics

China operates the world's second-largest economy and has experienced rapid economic transformation over the past four decades. The economy is characterised by a blend of state-controlled enterprises and market-oriented reforms, with the government maintaining significant control over key sectors including banking, telecommunications, and energy, while the number of private enterprises have also increased rapidly in the 21st century. China's Belt and Road Initiative has expanded its global economic influence through massive infrastructure investments across Asia, Africa, and Europe.

The political system is dominated by the Chinese Communist Party, which maintains centralised control over policy making and implementation. President Xi Jinping has consolidated power significantly since 2012, emphasising the party's role in all aspects of governance, and there are significant constraints on political expression and civil liberties.

China's financial system remains largely state-controlled, with the four largest commercial banks owned by the government. The country has been working to internationalise the yuan and reduce dependence on the US dollar in international trade. However, capital controls, restricted financial markets, and limited transparency create both opportunities and challenges for illicit financial flows.

Themis Expert View

WRITTEN BY:

Emily Hsu

Environmental and Financial Crime Researcher

China presents a complex and evolving financial crime risk landscape shaped by its unique political-economic system, rapid technological development, and growing global economic integration. The 2019 FATF evaluation recognised China's progress in strengthening its anti-money laundering framework, but significant vulnerabilities remain that create both domestic and international financial crime risks.

Key areas of concern include the prevalence of corruption despite ongoing anti-corruption campaigns, the rapid growth of digital payment systems that outpace regulatory oversight, and the use of Chinese financial networks for international money laundering operations. The country's capital controls, while limiting some money laundering risks, also create incentives for underground banking systems and informal value transfers that facilitate illicit flows.

China's role as a global manufacturing hub creates particular vulnerabilities around trade-based money laundering, intellectual property theft, and sanctions evasion. The country's significant state-owned enterprise sector, combined with limited transparency in beneficial ownership (BO) structures, creates opportunities for corruption and illicit enrichment by politically connected individuals.

The emergence of China as a major player in cryptocurrency mining and trading has created new risks, particularly around sanctions evasion and capital flight. Meanwhile, the government's development of a central bank digital currency (CBDC) represents both an opportunity to enhance transaction monitoring and a potential tool for state control over financial flows.

International cooperation remains challenging due to political sensitivities and differences in legal systems. However, China's integration into the global financial system means that Chinese financial crime risks have significant international implications, particularly for correspondent banking relationships and cross-border trade finance.

- MODERN SLAVERY & HUMAN TRAFFICKING
- MONEY LAUNDERING
- ENVIRONMENTAL CRIME
- CYBERCRIME
- FINANCIAL SECRECY
- SANCTIONS EVASION
- FRAUD
- BRIBERY & CORRUPTION
- DRUG & ARMS TRAFFICKING
- TERRORIST FINANCING

Regulatory Overview

Primary Anti-Financial Crime Regulators and Agencies:

- **People's Bank of China (PBOC):** Central bank and primary AML/CFT regulator; houses the China Anti-Money Laundering Monitoring and Analysis Centre (CAMLMAC) which serves as the Financial Intelligence Unit (FIU).
- **China Banking and Insurance Regulatory Commission (CBIRC):** Supervises banks and insurance companies for AML/CFT compliance.
- **China Securities Regulatory Commission (CSRC):** Regulates securities markets and investment firms for financial crime prevention.
- **Ministry of Public Security:** Leads criminal investigations and law enforcement activities.
- **Supreme People's Procuratorate:** Handles prosecution of financial crimes.
- **National Supervisory Commission:** Anti-corruption agency with broad investigative powers.
- **State Administration of Foreign Exchange (SAFE):** Monitors foreign exchange transactions and enforces capital controls.
- **Ministry of Commerce:** Oversees foreign investment and trade-related compliance.

Primary Anti-Financial Crime Legislation:

- **Anti-Money Laundering Law (2006, amended 2024):** Foundation of China's AML/CFT framework.
- **Criminal Law:** Defines money laundering and other financial crimes as criminal offences.
- **Counter-Terrorism Law (2015):** Includes terrorist financing provisions.
- **Cybersecurity Law (2017):** Addresses cyber-enabled financial crimes.
- **Data Security Law (2021):** Governs data protection and cross-border transfers.
- **Anti-Foreign Sanctions Law (2021):** Provides framework for countering foreign sanctions.

Financial Action Task Force Assessment

China underwent its most recent FATF Mutual Evaluation in 2019, with the final report recognising progress in strengthening the country's AML/CFT framework while identifying significant areas for improvement. China was placed in enhanced follow-up (with the most recent review undertaken in 2021) and has submitted progress reports to address technical and effectiveness deficiencies.

Category	2019 FATF Mutual Evaluation	2021 FATF Follow-Up Report
Overall Assessment	China has a well-established domestic framework for AML/CFT cooperation and coordination; however, improvements are needed to ensure that authorities are adequately accessing and using financial intelligence.	China has addressed some of the technical compliance deficiencies but remains in enhanced follow-up.
Technical Compliance Ratings	**Compliant:** 7 Recommendations **Largely Compliant:** 15 Recommendations **Partially Compliant:** 12 Recommendations: • R. 3: Money laundering offence • R. 6: Targeted financial sanctions – terrorism and terrorist financing • R. 8: Non-profit organisations • R. 12: Politically exposed persons • R. 15 New technologies • R. 16: Wire transfer • R. 18: Internal controls and foreign branches and subsidiaries • R. 26: Regulation and supervision of financial institutions • R. 28: Regulations and supervision of DNFBPs • R. 29: Financial intelligence units • R. 34: Guidance and feedback • R. 35: Sanctions • R. 38: Mutual legal assistance – freezing and confiscation **Non Compliant:** 6 Recommendations • R. 7: Targeted financial sanctions – proliferation • R. 22: DNFBPs: Customer due diligence • R. 23: DNFBPs – other measures • R. 24: Transparency and BO of legal persons • R. 25: Transparency and BO of legal arrangements • R. 28: Regulation and supervision of DNFBPs	**Compliant:** 9 Recommendations **Largely Compliant:** 22 Recommendations **Partially Compliant:** 3 Recommendations: • R. 6: Targeted financial sanctions – terrorism and terrorist financing • R. 12: Politically exposed persons • R. 35: Sanctions **Non Compliant:** 6 Recommendations • R. 7: Targeted financial sanctions – proliferation • R. 22: DNFBPs: Customer due diligence • R. 23: DNFBPs – other measures • R. 24: Transparency and BO of legal persons • R. 25: Transparency and BO of legal arrangements • R. 28: Regulation and supervision of DNFBPs
Key Risks Identified	- Main proceeds-generating predicate crimes are illegal fundraising, drug trafficking, corruption and bribery, tax crimes, counterfeiting of products, and gambling - Terrorist attacks in the northwest province of Xinjiang - Banks are highly vulnerable to abuse with respect to ML and TF, especially due to the volume of activity and rapid increase in online lending entities via mobile phone platforms - Abuse of legal persons as a method of laundering illicit proceeds	
Strengths	- Understanding of ML/TF risks - Capable law enforcement authorities - Availability and application of effective, proportionate, and dissuasive sanctions for ML - Institutional framework for investigating and prosecuting TF activities	- Measures to expedite foreign seizing, freezing and confiscation requests - Platform for collecting and sharing suspicious transaction reports - FIs' internal measures on countering ML/TF
Areas for Improvement	- Access and use of financial intelligence by authorities - Scope of TF targeted financial sanctions - FIs understandings and mitigation of their risks relating to ML and TF - Supervision of DNFBP sector - Handling of mutual legal assistance and extradition requests - Coverage of PEPs - Registering and retaining BO information	- Scope of TF targeted financial sanctions - Supervision of DNFBP sector - Coverage of PEPs - Registering and retaining BO information

Financial Crime Risk Matrix

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Modern Slavery & Human Trafficking	High	Global Organized Crime Index 2024 see here* Human Trafficking: 7 / 10 Human Smuggling: 6.5 / 10 **Global Crime Index Score is on a 0-10 scale, with 0 being non-existent crime to 10 being severe influence.* US Department of State 2024 Trafficking in Persons Report see here* Tier 3: The Government of the People's Republic of China (PRC) does not fully meet the minimum standards for the elimination of trafficking and is not making significant efforts to do so.	Manufacturing, construction, domestic work, forced labour, online fraud centres, fishing	Migrant workers from Southeast Asia are exploited in Chinese labour markets, and there is also domestic human trafficking and forced labour
Money Laundering	High	Basel AML Index 2024 see here* 10 / 7.27 (Ranked 11th of 152 countries) **Basel AML Score is on a 0-10 scale, with 10 representing the maximum risk.* Global Organized Crime Index 2023 see here* Financial Crime: 7.5 / 10 AML Resilience: 6.5 / 10 **Global Organized Crime Index Score is on a 0-10 scale, with 0 denoting non-existent crime and 10 severe influence.*	Banking, real estate, trade finance, underground banking, cryptocurrency	Global, but particularly Hong Kong and Macau
Environmental Crime	High	Global Organized Crime Index 2023 see here* Flora Crimes: 8.5 / 10 Fauna Crimes: 9 / 10 Non-Renewable Resource Crimes: 6 / 10 **Global Crime Index Score is on a 0-10 scale, with 0 being non-existent crime to 10 being severe influence.*	Mining, timber, wildlife trade, fishing, manufacturing	China imports large volumes of endangered species from Southeast Asia, South America, and Africa, such as rosewood and exotic wildlife. It is also involved in illegal mining operations, notably in Africa

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Cybercrime	High	National Cyber Security Index see here* 60/100 (Ranked 49) **Index measures the preparedness of countries to prevent cyber threats, with 100 representing the highest level of cybersecurity readiness* Global Organized Crime Index 2023 see here* Cyber-Dependent Crimes: 8.5 / 10 **Global Crime Index Score is on a 0-10 scale, with 0 being non-existent crime to 10 being severe influence.*	Technology, tele-communications, banking, critical infrastructure, government	China has been accused of sponsoring hacking activities abroad, and there cybercrimes are also a growing problem domestically
Financial Secrecy & Tax Crime	High	Financial Secrecy Index 2025 see here* 70/100 (Ranked 12 of 141 countries) **Secrecy index measures the level of financial secrecy, with 0 meaning no secrecy and 100 meaning maximum secrecy.* Corporate Tax Haven Index 2025 see here* 62/100 (Ranked 16 of 70 countries) **Corporate Tax Haven Index ranks the world's biggest enablers of global corporate tax abuse, with scores ranging from 0 (no room for tax abuse) to 100 (unlimited room for tax abuse).*	Private banking, trust services, offshore entitiess	Hong Kong, Macau, Singapore, tax havens, offshore financial centres
Sanctions Evasion	High	China faces extensive international sanctions and has developed sophisticated networks to evade restrictions, particularly related to technology transfers and dual-use goods.	Technology, banking, shipping, energy, defense	Russia, Iran, North Korea, Myanmar

*Methodology: Each financial crime risk rating is derived from a combination of globally recognised indices and supplementary risk factors. Each index score is normalised and translated into a Red-Amber-Green (RAG) rating. Specifically, jurisdictions or entities are grouped based on their position within the distribution of index values, with the top, middle, and bottom third of scores per index corresponding respectively to Green, Amber, and Red (e.g. a 5/10 rating in one index would be equivalent to a 12/24 rating in another). Additional risk factors — such as enforcement actions, FATF evaluations, and our own Themis internal intelligence — also influence the final RAG classification through an overlay and adjustment process.

Bribery & Corruption	Medium-High	Transparency International Corruption Perceptions Index 2024 see here* 43/100 (Ranked 76th of 180 countries) **Transparency International Corruption Perceptions Index score is the perceived level of public corruption, where 0 means highly corrupt and 100 means very clean.* Trace 2024 Bribery Risk Matrix see here* 59/100 (Ranked 142 of 194 countries) **Trace measures business bribery risk with a lower score indicating a lower bribery risk, while a higher score indicating a higher bribery risk.* Global Organized Crime Index 2023 see here* Government Transparency and Accountability: 4 / 10 State-Embedded Criminality: 7 / 10 Private Sector Criminality: 7 / 10 **Global Crime Index Score is on a 0-10 scale, with 0 being non-existent crime to 10 being severe influence.*	Construction, infrastructure, state-owned enterprises, healthcare, real estate	Belt and Road Initiative countries
Terrorist Financing	Medium-High	Global Terrorism Index (GTI) 2024 see here* Overall Score: 1.863 / 10 (Ranked 49th of 163 countries) China has a moderate risk of domestic terrorism attacks, but the FATF has noted its financial systems are vulnerable to terrorist financing. **The GTI scores each country on a scale from 0 to 10; where 0 represents no impact from terrorism and 10 represents the highest measurable impact of terrorism.*	Banking, charities/ NPOs, online platforms, informal value transfer	Central Asia, Middle East, Southeast Asia
Drug and Weapons Trafficking	Medium-High	Global Organized Crime Index 2023 see here* Heroin Trade: 6.5 / 10 Cocaine Trade: 3.5 / 10 Cannabis Trade: 4.5 / 10 Synthetic Drug Trade: 8 / 10 Arms trafficking: 3 / 10 **Global Crime Index Score is on a 0-10 scale, with 0 being non-existent crime to 10 being severe influence.*	Chemical manufacturing, logistics, shipping, border regions	Drugs transiting to China through the Golden Triangle, or from Afghanistan, Pakistan, Iran, and South America, sometimes onwards to final markets in Australia
Fraud	Medium-High	According to the Global Organized Crime Index, fraud is pervasive in China, often in concert with corruption and bribery.	Technology, telecommunications, e-commerce, banking, investment	International fraudsters operating in cross-border schemes may be involved. China is also one of the world's largest sources of counterfeit items

Areas of Financial Crime Vulnerability

- **Underground Banking Networks:** Extensive informal value transfer systems operate alongside formal banking, facilitating capital flight, sanctions evasion, and money laundering with limited regulatory oversight and investigation capabilities.
- **State-Controlled Financial System:** Dominance of state-owned banks and enterprises creates opacity around politically connected transactions and BO structures and challenges for independent regulatory oversight and enforcement.
- **Manufacturing and Trade Hub Status:** China's role as the "world's factory" creates extensive opportunities for trade-based money laundering, including over/under-invoicing, phantom shipments, and commodity price manipulation across global supply chains.
- **Capital Control Circumvention:** Strict foreign exchange controls create strong incentives for underground banking, cryptocurrency adoption, and complex corporate structures designed to move money offshore illegally.
- **Digital Payment System Rapid Growth:** The massive scale and rapid innovation in mobile payments and digital financial services has outpaced regulatory frameworks, creating vulnerabilities for fraud, sanctions evasion, and money laundering.
- **Belt and Road Initiative Complexity:** Massive infrastructure investments across developing countries create opportunities for corruption, sanctions evasion, and money laundering through complex multi-jurisdictional project structures with limited transparency.

Financial Crime Risk In-Depth

01 Modern Slavery & Human Trafficking: High Risk

Forced labour remains extensive across multiple sectors, including manufacturing, construction, and domestic work. The government's policies in Xinjiang have created systematic forced labour affecting Uyghurs and other ethnic minorities. Cross-border trafficking involves Chinese victims trafficked abroad and foreign victims brought to China. Recent developments include the use of overseas criminal compounds for online fraud operations that trap thousands of workers in forced labour conditions across Southeast Asia.

02 Money Laundering: High Risk

China faces significant money laundering threats primarily from corruption proceeds, fraud, and illegal capital flight. Underground banking networks facilitate much of this activity, with estimates suggesting informal value transfers worth hundreds of billions annually. Trade-based money laundering is particularly prevalent given China's dominant role in global trade. Key typologies include over/under-invoicing of goods, phantom shipments, and manipulation of commodity prices. The banking sector has strengthened AML controls significantly, but non-bank financial institutions and cross-border correspondent banking relationships remain vulnerable.

03 Cybercrime: High Risk

China is both a major source and target of cybercrime, with state-sponsored groups conducting extensive economic espionage and private criminal networks running sophisticated fraud operations. Telecommunications fraud has reached epidemic proportions, with criminal networks often operating from overseas bases targeting Chinese diaspora communities globally. Cryptocurrency fraud and investment scams generate billions in proceeds annually. The country's advanced technology sector creates both opportunities and vulnerabilities for cyber-enabled financial crimes.

04 Environmental Crime: High Risk

China's rapid industrialisation and huge domestic market drive extensive environmental crime, including illegal logging, wildlife trafficking, and illegal mining. The country is a major destination for trafficked wildlife products, particularly ivory, rhino horn, and pangolin scales. Illegal fishing operations extend globally, often involving complex corporate structures to evade oversight. Domestic environmental crimes include illegal dumping of hazardous waste and unauthorised mining operations that generate significant illicit proceeds.

05 Financial Secrecy & Tax Crime: High Risk

While China has made progress on BO transparency for domestic entities, complex ownership structures involving Hong Kong, Macau, and offshore jurisdictions remain common. State-owned enterprises and party-connected individuals frequently use layered corporate structures to obscure true ownership. Special Economic Zones and Free Trade Zones offer enhanced financial secrecy that can be exploited for illicit purposes. The lack of comprehensive public registries and limited international information sharing creates ongoing vulnerabilities.

06 Sanctions Evasion: High Risk

China faces extensive international sanctions and has developed sophisticated evasion networks, particularly for technology transfers and dual-use goods. Chinese companies regularly engage in sanctions-busting activities benefiting Russia, Iran, and North Korea. Key methods include use of shell companies, re-routing through third countries, and exploitation of correspondent banking relationships. The development of alternative payment systems and increased use of cryptocurrency facilitate sanctions evasion activities.

07 Fraud: Medium-High Risk

China faces a multifaceted fraud environment, spanning traditional internal collusion and sophisticated digital schemes. Internally, enterprises commonly encounter fraud involving employee-vendor collusion ranging from inflated procurement and fictitious services to abuse of marketing budgets, which highlights weak internal controls and oversight. Simultaneously, telecom and cyber fraud cases have surged, and in the digital realm, scams such as false investment schemes, fake logistics, click-farm jobs and credit repair fraud remain pervasive, particularly among younger adults.

08 Terrorist Financing: Medium-High Risk

Terrorist financing risks are primarily concentrated in western regions with ethnic tensions and cross-border connections to Central Asian extremist groups. Online platforms and mobile payment systems present emerging risks for terrorist financing, whilst traditional hawala networks persist in border regions. The government's extensive domestic surveillance capabilities limit domestic terrorist financing, but international cooperation on cross-border cases remains challenging due to political sensitivities.

09 Bribery & Corruption: Medium-High Risk

Despite extensive anti-corruption campaigns since 2012, corruption remains systemic across government and state-owned enterprises. Construction, infrastructure development, and public procurement present the highest risks. The Belt and Road Initiative has created new opportunities for corruption involving Chinese companies and officials in overseas projects. Party-connected individuals continue to exploit their positions for personal enrichment, often using complex offshore structures to hide assets. Recent regulatory crackdowns on technology and private equity sectors have revealed extensive corrupt relationships between officials and business leaders.

10 Drug & Weapons Trafficking: Medium Risk

China serves as a major source of fentanyl precursors and synthetic drugs destined for international markets, particularly North America and Europe. The country's extensive chemical manufacturing industry and limited oversight of precursor chemicals enable illicit drug production. Traditional drug trafficking through border regions remains active, particularly involving heroin from the Golden Triangle region. Money laundering from drug proceeds occurs primarily through underground banking and trade-based methods.

Case Study

Xinkangjia and the DGCX Ponzi Scheme

In June 2025, Xinkangjia DGCX, a purported online commodities investment platform, collapsed abruptly, freezing user assets and vanishing with an estimated 13 billion RMB (~$1.8 billion USD), defrauding over 2 million investors. Marketed as the official Chinese substation of the Dubai Gold and Commodities Exchange (DGCX) — a claim publicly denied by DGCX)—Xinkangjia fabricated legitimacy through forged contracts, fake partnerships with state-owned giants like PetroChina and COSCO, and professional-looking interfaces simulating real-time commodities trading.

Behind the operation was Huang Xin, the alleged founder who fled overseas shortly before the collapse. The fraud operated as a hybrid Ponzi scheme with a multi-level marketing (MLM) structure, built on blockchain infrastructure and using USDT (Tether) for transactions. New users were onboarded via invitation codes and prompted to convert RMB to USDT, which they deposited to assigned addresses, with users never holding their own private keys. The platform displayed fake market dashboards, promised daily returns of up to 2%, and promoted slogans like "double your money in 7 days." In its final days, Xinkangjia raised the withdrawal threshold drastically, introduced new bait campaigns like "invest 500,000 and win a Tesla," and reportedly funnelled 1.8 billion USDT into offshore accounts before vanishing.

Why This Case Matters: The Xinkangjia case highlights the increasing complexity and psychological manipulation underpinning modern digital Ponzi schemes in China. It underscores vulnerabilities in financial literacy among underbanked and elderly populations, and reveals systemic regulatory blind spots, despite prior warnings from local financial authorities. It also exposes how digital assets and blockchain infrastructure, without adequate oversight, can be weaponised to simulate legitimacy and obscure fraud at scale. The platform's success in projecting state-linked credibility using fake partnerships and forged documentation reflects a broader challenge: the blurring of lines between state and private actors in the public's perception, which scammers exploit with alarming ease.

KEY TAKEAWAYS:

- **Digital veneer and offline hustle:** Xinkangjia combined on-chain complexity with grassroots-level promotion (WeChat groups, seminars), effectively scaling its scam across vulnerable demographics.
- **MLM meets DeFi:** The case demonstrates how pyramid schemes are evolving through digital tokens and "investment" platforms that mimic legitimate financial interfaces.
- **Due diligence failure:** Despite risk alerts from local authorities, the scam thrived due to lack of centralised enforcement, limited digital asset regulation, and rampant misinformation.
- **Ponzi camouflage:** Promises of fixed high returns, tiered bonuses, and "government-endorsed" branding should serve as red flags for fraud, especially in the context of digital assets.

Case Study

The Sinaloa Cartel and San Gabriel Valley Money Laundering Ring

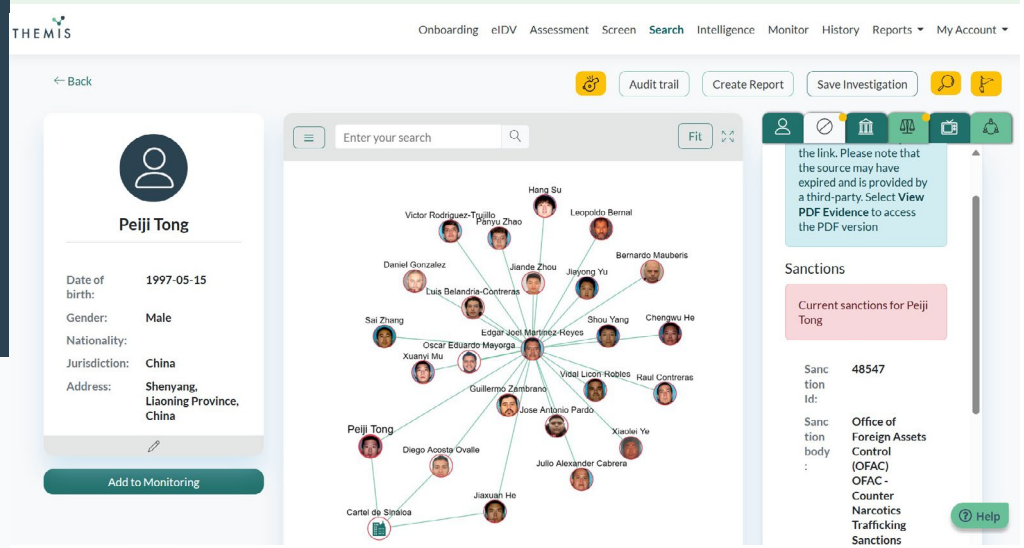
In 2024, US federal prosecutors indicted 24 individuals for orchestrating a sophisticated transnational money laundering scheme linking Mexico's Sinaloa cartel with a Chinese underground banking network based in California's San Gabriel Valley. The group, led by Edgar Joel Martinez-Reyes and Peiji Tong, allegedly laundered over $50 million in drug proceeds from the sale of fentanyl, methamphetamine, and cocaine in the US. The core mechanism involved matching the cartel's surplus of bulk US dollars with wealthy Chinese nationals seeking to circumvent China's capital controls, which limit citizens from legally moving more than $50,000 per year abroad.

The laundering process worked as follows: a Chinese client in need of US dollars contacted a broker in California. At the broker's direction, drug money would be delivered to the Chinese buyer's representative in the US. These dollars were then used to buy consumer goods or precursor chemicals from Chinese manufacturers. The products were shipped to Mexico, where they were sold by the cartel for pesos or used to manufacture synthetic drugs, thus completing the cycle. According to prosecutors, the Chinese-American network offered significantly lower laundering commissions (0.5%–2%) than traditional channels, creating a lucrative, high-volume system.

Why This Case Matters: This case exposes a growing convergence between narco-trafficking and underground Chinese capital flight networks, revealing how global financial restrictions and opaque supply chains can be exploited to sustain illicit economies. It underscores the evolution of money laundering from legacy financial channels to transnational barter-style systems built on dual needs: drug cartels needing to repatriate cash discreetly, and Chinese elites seeking access to US assets. The use of legitimate-seeming trade flows, like electronics or chemical shipments, illustrates how trade-based money laundering has become a favoured technique to obscure illicit fund flows across borders.

KEY TAKEAWAYS:

- **Underground convergence:** The case reveals a symbiotic relationship between Mexican drug cartels and Chinese underground banking networks, rooted in mutual need and efficiency.
- **Trade-based laundering:** Physical goods became the medium to return value to the cartel in Mexico, evading detection through trade routes.
- **Low-fee competition:** The San Gabriel Valley network undercut traditional laundering fees, offering streamlined, scalable operations that attracted high-volume criminal clients.
- **Capital control exploitation:** China's strict currency export rules continue to fuel black-market demand for US dollars, inadvertently supporting criminal laundering schemes.



Key Financial Crime Watchpoints

The following watchpoints highlight common financial crime risk indicators to lookout for as regards clients, partners, suppliers, and broader business transactions and relationships. They are designed to support client risk assessments, enhanced due diligence and transaction monitoring by identifying patterns frequently associated with financial crime in China.

- **Complex Corporate Ownership Structures:** Multiple layers of Chinese entities, often involving Hong Kong and offshore companies, with nominee shareholders and directors used to obscure BO and facilitate illicit fund flows, particularly for sanctions evasion and corruption.
- **Underground Banking Indicators:** Rapid, high-volume transactions through informal networks, trade invoicing anomalies, cash-intensive remittance businesses, and cryptocurrency transactions that circumvent formal banking channels and capital controls.
- **Belt and Road Initiative Transaction Anomalies:** Infrastructure project financing involving unusual routing through third countries, inflated contract values, unexplained cost variations, and payments to entities with no clear connection to project activities.
- **Trade-Based Money Laundering Red Flags:** Significant over/under-invoicing of goods, phantom shipments, commodity transactions with pricing inconsistent with market rates, and frequent use of middleman companies in trade finance documentation.
- **State-Connected Entity Risks:** Transactions involving state-owned enterprises or politically connected individuals, particularly those involving overseas investments, real estate purchases, or complex corporate structures that may facilitate corruption or sanctions evasion.
- **Digital Payment System Exploitation:** Large-value transfers through mobile payment platforms, rapid movement of funds through multiple digital wallets, use of digital payments to circumvent banking oversight, and integration with cryptocurrency exchanges for cross-border transfers.

How Themis Can Help

Financial crime has evolved faster than traditional systems. Themis delivers a new AI-powered, end-to-end platform purposebuilt to help businesses detect, prevent, and respond to threats in real time. A modular solution that fuses advanced analytics, automation, and proprietary intelligence to tackle risk at scale and fast. As financial crime becomes more complex, Themis delivers clarity, speed, and impact. This isn't an evolution. It's the platform the future demands — powered by data, powered by Themis.

Themis aims to be a leader in applying AI-led solutions to the problems of financial crime, and we are uniquely placed to do so. With strong working relationships with governments and businesses of many shapes and sizes, our software is developed with the needs of the whole financial crime compliance ecosystem in mind. By combining a focus on innovative technology with leading human intelligence and insight, Themis is capable of not only meeting those needs as they currently are but also anticipating them as they evolve in an uncertain future.

Our Reports and Services

Enjoyed this briefing? Keen for a more detailed analysis that's specific to your business? We deliver longer, bespoke reports and executive briefings about specific countries or sectors. Whether you're investing in new markets, expanding your own footprint or ensuring your financial crime country risk assessments align with the Wolfsberg Group's principles, our Risk Intelligence team can help. We specialise in complex, strategic projects where financial crime risks are new, emerging, or poorly understood.

Get in touch to find out more.

Our Team of Experts

Nadia O'Shaughnessy
Head of Insight
nos@wearethemis.com

Olivia Dakeyne
Principal, Research
od@wearethemis.com

Eliza Thompson
Financial Crime Researcher
et@wearethemis.com

Henry Wyard
Senior Policy Analyst
hjw@wearethemis.com

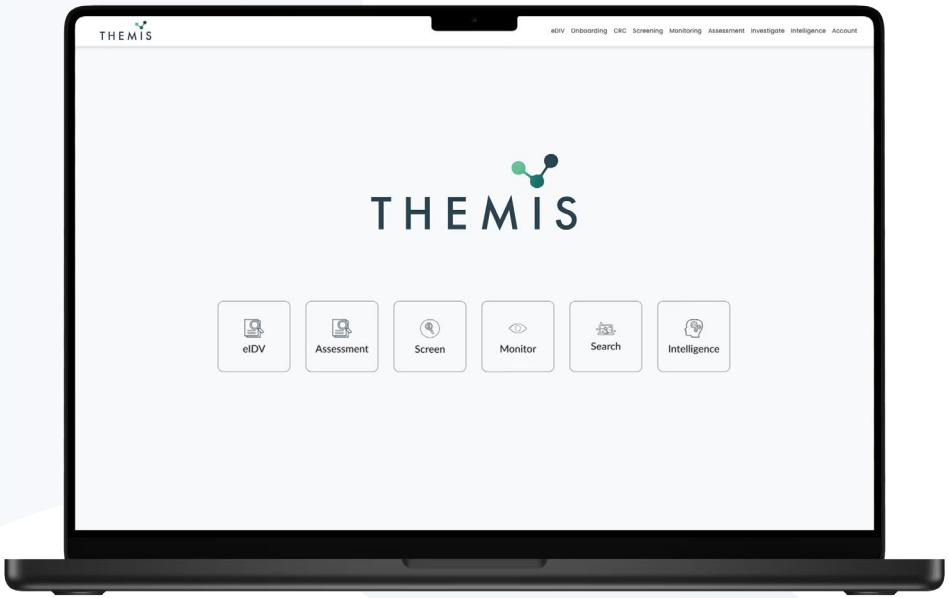
Nikhil Gandesha
Global Financial Crime Training Lead
ng@wearethemis.com

Emily Hsu
Financial and Environmental Crime Researcher
eh@wearethemis.com

Discover Other Country Risk Briefings

Research-driven analysis that informs and inspires action to tackle financial crime

Discover all



THEMIS

UK: +44 (0) 20 8064 1724 | UAE: +971 (0) 58 526 8765

info@wearethemis.com

www.wearethemis.com

Certified B Corporation