

**Converging Criminal Enterprises:
Chinese Money Laundering Networks
and Cartel Financing
in the U.S. Financial System**

Written Testimony

of

John A. Cassara

Presented to the

Subcommittee on Oversight & Investigations

U.S. House Financial Services Committee

June 9, 2026

Thank you, Chairman Meuser, Ranking Member Green, and distinguished members of the Subcommittee on Oversight & Investigations of the U.S. House Financial Services Committee, for the opportunity to testify today on “Converging Criminal Enterprises: Chinese Money Laundering Networks and Cartel Financing in the U.S. Financial System.”

Before addressing Chinese money laundering networks, I would like to briefly discuss our efforts to combat money laundering in general through the U.S. financial system.

I have both investigated and analyzed international money laundering for well over 30 years. With that perspective, I can definitively state that based on the metrics that matter (forfeitures and convictions), our anti-money countermeasures have failed. Both our legislative fixes and enforcement actions are not putting a dent in the growing problem. I’m not alone in my observations. For example, Ron Pol, a respected anti-money laundering researcher claims, “Anti-money laundering legislation is the least effective of any anti-crime measure, anywhere.”ⁱ

Bottom Line Metrics

Estimating the magnitude of international money laundering in general is fraught with difficulties. By definition, money laundering is opaque and hidden. The Financial Action Task Force (FATF) states, “due to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year.”

With that caveat in mind, the International Monetary Fund (IMF) has estimated that money laundering comprises approximately two to five percent of the world’s gross domestic product (GDP) every year. Money laundering experts frequently use the IMF estimate when they need to discuss the magnitude of money laundering.

In 2025, global GDP was approximately \$117 trillion. So, in very round numbers, the total amount of money laundered worldwide annually is somewhere in the vicinity of roughly \$3 to \$5 trillion. Of course, the estimate could be far higher depending on what is included in the count. For example, I don’t believe the IMF estimate includes tax evasion, forms of trade fraud, or underground financial systems. Illicit capital flight is another category which could be considered money laundering but is generally ignored.

Out of the trillions of dollars that are laundered every year, how much of the proceeds of crime are actually seized and forfeited? According to the UNODC, the answer is less than one percent.ⁱⁱ It bears repeating; we successfully seize and forfeit less than one percent of the proceeds of crime that are laundered globally every year. The U.S. has approximately the same failure rate.

The other bottom-line metric that matters is the number of successful investigations, prosecutions, and convictions. While statistics of this nature vary markedly from country to country, are open to question, and sometimes do not include the money-laundering activities of criminals convicted on other charges, the sobering fact is that for a money launderer to be caught and convicted today, he or she has to be either very stupid or very unlucky.

In sum, primarily because of the magnitude of the problem, money laundering enforcement fails 99.9 percent of the time. Or as longtime financial crime expert Raymond Baker notes, “Total failure is just a decimal point away.”ⁱⁱⁱ

Our failure has real consequences. The pernicious criminal activity behind the dirty money affects the peace and security of nations, societies as a whole, threatens citizens’ safety and community stability. The tens of trillions of dollars that are the product of transnational crime corrupt segments of society, our politics, and the global financial order.

In the United States, it is estimated that approximately \$730 billion is laundered annually, equivalent to 2.5 per cent of our GDP.^{iv} (However, I believe that the proceeds of illicit crime in the United States are well over \$1 trillion annually. Once again, it depends what is included in the count). The criminality, or specified unlawful activities (SUAs) that generate the illicit funds affect all Americans, our families and our communities. Your constituents face increasing threats related to narcotics trafficking, e-commerce, and mobile payment fraud and scams, criminal activity associated with human trafficking, skyrocketing government service fraud, the proliferation of counterfeit goods, and many other threats both at the national and local level.

Meanwhile, anti-money laundering enforcement and compliance costs are similarly skyrocketing. Anti-money laundering (AML) and financial crime compliance costs U.S. financial institutions an estimated \$46 billion annually, with global spending exceeding \$206 billion.^v For individual institutions, these costs consume 3% to 5% of average annual revenue, ranging from \$500,000 for small community banks to upwards of one billion dollars for massive global banks. These costs are passed on to the consumer.

What is the return on these expenditures? The question is rarely asked but should be. Between the Department of Justice and the Treasury Department, total national forfeiture deposits regularly range between \$2 - \$4 billion annually. Adding in state and local forfeitures does not make much of an impact. So, in other words, commercial anti-money laundering expenditures alone are about twenty times higher than the illicit proceeds recovered. The numbers are even worse because we also have to add to the cost equation incalculable anti-money laundering enforcement and regulatory expenditures at the federal, state and local levels.

While the focus of this hearing is not about reimagining our anti-money laundering efforts, we are talking about threats to the U.S. financial system. I wish to emphasize that there are a number of important steps we can take. I discuss many of them in my book [*Money Laundering and Illicit Financial Flows*](#), (Amazon / Kindle Direct Publishing 2020).

Chinese Money Laundering Networks

The above metrics demonstrate both the magnitude of international money laundering and our failures to address it. There are many causes. An increasingly important reason for the growth in many sectors of transnational crime that we continue to ignore at our peril is that the People's Republic of China has become the biggest transnational criminal actor and money laundering threat.

My most recent book is [*China – Specified Unlawful Activities: CCP/Inc., Transnational Crime and Money Laundering*](#) (Amazon / Kindle Direct Publishing 2023). I wrote the book at the end of my long anti-money laundering career because I am simply staggered by facts and observations that demonstrate China's criminal hegemony and how it launders illicit proceeds. Similar to North Korea, today's communist China is a corrupt party-state regime with a significant crime portfolio. Criminal activity has seemingly become part of the CCP's overall strategy to grow its power.

The CCP/Inc. subtitle of the book makes clear that I am talking about communist China's transnational crime and money laundering - not the Chinese people. In many ways, they are the biggest victims of the CCP regime.

Simply referring to China alone or the CCP by itself is ambiguous, unfair, and inaccurate. To be clear, what I am referring to in my book and in this testimony is the centralized autocracy of the CCP and its heretofore unexamined linkages with illicit crime, corruption, and money laundering. Although I will use the term 'China,' and 'Chinese' in this testimony, that is solely in reference to the Party's dominance of the PRC's governance apparatus, and should not be misconstrued to be a condemnation of Chinese culture or the Chinese people, who have no choice in what regime they live under. The "Inc." is a term that signifies how the Chinese state has leveraged its industrial, high tech, global trading, manufacturing might, and illicit

connections to turn the country into an economic superpower. So, I will use “CCP Inc.” as a general descriptor of the subject under discussion.

Specified Unlawful Activities

In my book, I examine perhaps the 12 most significant sectors of transnational crime. In 11 of the 12 categories, CCP/Inc. is the world’s leading criminal actor. The 12 categories of crime are:

- Counterfeit goods
- Intellectual property theft and trade secrets
- Human trafficking, smuggling and forced labor
- Narcotics trafficking
- Wildlife trafficking
- Illegal logging
- Illegal fishing
- Illicit tobacco
- Trade fraud
- Arms trafficking and WMD proliferation
- Organ harvesting
- Corruption

Each of the above categories of crime are also “specified unlawful activities” (SUAs) or predicate offenses to charge money laundering. I acknowledge that using SUAs and the estimates of illicit funds generated is not an ideal way of assessing money laundering. Measuring the scale of illicit funds derived from criminal or illegal activity is challenging. But there is a strong consensus regarding China’s involvement.

Putting things in context, let’s use \$4 trillion as a rough estimate of the annual magnitude of international money laundering. Using recognized estimates^{vi} put forward by the Washington D.C.-based non-profit Global Financial Integrity (GFI) and other sources, a solid argument can be made that by examining China’s leading role in the above listed transnational SUAs, China is responsible for introducing and laundering approximately \$2 trillion dollars of illicit proceeds

into the world's economy every year.^{vii} In other words, China is responsible for approximately one-half of the money laundered throughout the world every year as measured by SUAs.

The number is staggering. It bears repeating. As measured by the largest categories of SUAs for transnational crime, CCP Inc. and its associated actors are responsible for about half of the money laundered internationally each year. No other country even comes close.

My book, *China – Specified Unlawful Activities*, examines each of the above listed SUAs and quotes recognized sources estimating the amount of illicit proceeds generated.

I believe both the administration and Congress make a tremendous mistake if they focus on single issues such as Chinese involvement in the fentanyl trade or intellectual property theft. Instead, I urge we examine the *totality* of CCP/Inc.'s criminal actions, money laundering methodologies and enablers. They are intertwined and mutually supportive.

Having worked in the U.S. government as well as at one time being actively involved in the Financial Action Task Force (FATF), I understand the political hesitation to officially make the charge that CCP Inc. could be considered an ongoing criminal enterprise and the largest money laundering actor in the world. Generally speaking, both the international community and the U.S. government are silent on the magnitude of China's involvement in transnational crime and money laundering.

We shouldn't be silent. In my view, targeting CCP Inc. via coordinated and comprehensive law enforcement action, both within the United States and overseas, is where the Chinese Communist Party is most vulnerable. And we will not make progress in combatting international money laundering unless we honestly acknowledge the CCP threat and take coordinated and decisive enforcement action to deal with it.

CMLNs and Cartel Financing in the U.S. Financial System

On March 23, 2023, I testified before the U.S. House Committee on Financial Services' Subcommittee on National Security, Illicit Finance and International Financial Institutions. The topic of the hearing was, [“Follow the Money: The CCP's Business Model Fueling the Fentanyl Crisis.”](#) In that hearing, other witnesses and myself explained the Chinese supply chain of

fentanyl and precursors and how Chinese have become the “money launderers of choice for the cartels.” I will not repeat the details of the China/cartel relationship here.

Before I offer some observations about how Chinese-centric money laundering methodologies and enablers impact the U.S. financial system and bypass our traditional AML countermeasures, I would like to emphasize that we are witnessing a very active evolution in money laundering. Increasingly, money is no longer money in the conventional sense of the term. And the mantra of “follow the money” is not as central as in the past when illicit money does not move. It is value transfer without money movement. The dirty money stays in place.

Black market systems and ancient techniques of “value transfer” are infused and modernized with 21st century technology. For example, illicit funds are now being transferred via mobile payments, mirror swaps, digital assets, cryptocurrency transactions, decentralized finance (DeFi) platforms, end-to-end encryption-powered apps, and other novel digital-technological means that facilitate anonymity and underground criminality outside of regulated financial systems and our traditional Bank Secrecy Act anti-money laundering (AML) countermeasures.^{viii} Capital is being “swapped” for money or value in another location. Little if any “financial intelligence” results.

Just a few weeks ago, an [indictment](#)^{ix} was returned in the nearby Eastern District of Virginia *charging Ruhuan Zhen and Hongce Wu, both Chinese nationals, with conspiracy to commit money laundering in connection with transnational criminal organizations, including the Sinaloa Cartel and the Cartel de Jalisco Nueva Generación (CJNG).*

According to court documents, beginning in at least November 2016 and continuing to April 2025, Zhen, Wu, and their co-conspirators are alleged to have used a variety of secretive and clandestine methods, including mirror transfers, foreign bank accounts, encrypted communications applications, a serial-number verification system, and trade-based money laundering, to launder substantial volumes of narcotics proceeds and funds represented to be narcotics proceeds on behalf of transnational criminal organizations. The conspiracy is alleged to span the course of years with co-conspirators operating across the United States, Mexico, Latin America, China, and elsewhere, and involve drug proceeds stemming from the importation and sale of illicit narcotics, including cocaine and fentanyl.

Zhen and Wu were indicted on April 24, 2025, by a federal grand jury empaneled in Alexandria, Virginia, and remain at large.

The above case demonstrates how a variety of Chinese-centric money laundering methodologies and enablers both impact and skirt the U.S. financial system. In the balance of my testimony, I would like to explain some of the most prominent as well as call attention to a few new CCP/Inc-centric criminal activities, enablers, and laundering methods.

Money Laundering Methodologies and Enablers

In my book, *China – Specified Unlawful Activities*, I discuss a number of money laundering methodologies and enablers with “Chinese characteristics.” (The term Chinese characteristics is used by the CCP itself). Many examples are given. Collectively, they are intertwined in the CCP’s business model. Some of the methodologies I explore include Chinese underground banking or CUBS, capital flight, gambling, real estate, and the use of offshores and secrecy jurisdictions. Corruption can be both methodology and also a SUA. I also call corruption “the great enabler” for money laundering. Bribery is part of the CCP Inc. business model and gameplan. CCP Inc. has taken their domestic corruption and exported it overseas. The modus operandi abroad is using corruption and “corrosive capital” as instruments of foreign policy. This is further augmented by “elite capture” and sophisticated influence operations. This occurs in the United States and against American interests abroad. Other enablers I discuss in my book include Chinese organized crime, espionage, social monitoring, the promotion of Chinese control of Free Trade Zones (FTZs), lack of Chinese cooperation with international law enforcement, and poor Chinese money laundering compliance.

Methodologies that are intertwined with Chinese money laundering networks and cartel financing that are directly related to recent investigations are trade-based money laundering, black-market exchanges, capital flight, mirror swaps, and fei-chien or “flying money.” I will provide brief explanations of each.

Trade-based money laundering (TBML)

Perhaps the most extensive or widespread form of Chinese (and global) money laundering comes from “trade-mis-invoicing” or trade fraud. Trade fraud or customs fraud is a

SUA for money laundering. Depending on its form, it can also be a money laundering methodology. In fact, I believe it is the largest and most widespread methodology for both China and the world at large. It is also the least understood, recognized, and enforced.

For a detailed examination of TBML, please see my book *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*, Wiley, 2016.

Most forms of trade mis-invoicing revolve around invoice fraud and manipulation. Generally speaking, invoice fraud means the contents, description, and/or the value of goods is deliberately misrepresented. Sometimes this is done to facilitate simple customs fraud, i.e., minimize the payment of taxes and duties, avoid currency controls, or move capital or value offshore. International trade via invoice manipulation is also a very common means used by criminals and criminal organizations to illegally transfer value across international borders.

TBML is defined by the FATF as “the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.”^x The key word in the definition is *value*. Instead of following the money trail via cash or the electronic bits and bytes of a bank-to-bank wire transfer, with TBML we examine the shipments of commodities and trade goods. Their sale and transfer—real and fictitious—very effectively launders money, evades taxes and tariffs, and transfers value between cooperating parties in the transaction(s).

TBML is very broad. It includes customs fraud, tax evasion, export incentive fraud, value-added tax (VAT) fraud, capital flight or the transfer of wealth offshore, evading capital controls, barter trade, underground financial systems such as hawala and fei-chien (the Chinese “flying money” system), black market exchange systems, and even forms of commercial TBML such as trade diversion, transfer pricing, and abusive trade mis-invoicing.

For money launderers and terrorist financiers, transferring value via trade goods is particularly attractive because it generally does not trigger financial transparency reporting requirements or the filing of financial intelligence or, as it is commonly called in the U.S., “Bank Secrecy Act (BSA) data.” Financial intelligence promotes a degree of financial transparency and is our primary AML/CFT countermeasure.

The most common forms of trade mis-invoicing are:

John A. Cassara
www.JohnCassara.com

- Over and under invoice pricing
- Multiple invoicing for the same goods
- Falsely described goods
- Mis-representation of the quantity being shipped
- Mis-representation of voyage to disguise origin from sanctioned countries
- Mis-representation of shipment origin and voyage to evade customs duties

Most of the above are self-explanatory. But I do want to briefly explain how over and under invoicing is used to transfer value and launder money, because I will refer to this below when I discuss the Chinese underground “flying money” system.

The key element of this technique is the misrepresentation of trade goods to transfer value between the importer and exporter or settle debts/balance accounts between the trading parties. When an importer and exporter are working together, they can easily manipulate the invoice to reflect a price that does not adhere to true market value. The shipment (real or fictitious) of goods and the accompanying documentation provide cover for the transfer of money. Invoice fraud is generally considered customs fraud. And customs fraud is the primary predicate offense or specified unlawful activity in TBML cases.

What are the most common invoice scams? First, by under-invoicing goods below their fair market price, an exporter is able to transfer value to an importer while avoiding the scrutiny associated with more direct forms of money transfer. The value the importer receives when selling (directly or indirectly) the goods on the open market is considerably greater than the amount he or she paid the exporter.

For example, Company A located in China ships one million widgets worth \$2 each to Company B based in Mexico. On the invoice, however, Company A lists the widgets at a price of only \$1 each, and the Mexican importer pays the Chinese exporter only \$1 million for them. Thus, extra value has been transferred to Mexico, where the importer can sell (directly or indirectly) the widgets on the open market for a total of \$2 million. The Mexican company then has several options: it can keep the profits; transfer some of them to a bank account outside the

country where the proceeds can be further laundered via layering and integration; share the proceeds with the Chinese exporter (depending on the nature of their relationship); or even transfer them to a criminal organization that may be the controlling interest behind the business transactions.

To transfer value in the opposite direction, an exporter can over-invoice goods above their fair market price. In this manner, the exporter receives value from the importer because the latter's payment is higher than the goods' actual value on the open market.

Here is a simple way of looking at things:

To move money/value out:

- Import goods at overvalued prices or export goods at undervalued prices

To move money/value in:

- Import goods at undervalued prices or export goods at over-valued prices

Unfortunately, the magnitude of TBML has never been systematically examined by the FATF, international financial institutions (IFIs) —e.g., IMF or World Bank—or the U.S. government. Trade-based value transfer is also not closely examined by intelligence, law enforcement, and customs services. But some academics and non-profits have done very useful work examining TBML and estimating the extent of the challenge.

In the United States, Dr. John Zdanowicz, an early pioneer in the study of TBML, conducted research that identified glaring anomalies in U.S. trade data. For example, he found plastic buckets from the Czech Republic imported with the declared price of \$972 per bucket! Toilet tissue from China imported at the price of over \$4,000 per kilogram. Bulldozers shipped to Colombia at \$1.74 each! Why are non-industrial diamonds being exported to France for \$2.32 per carat but imported from South Africa for \$929,390.82 per carat? Dr. Zdanowicz compares the declared value of the trade good or commodity against true market value. By examining 2021 U.S. trade data, Dr. Zdanowicz found that approximately \$784 billion was moved into the U.S. via over-valued exports and under-valued imports. China was the trading partner for about \$85 billion of the total. Approximately \$640 billion was moved out of the U.S. via undervalued exports and over-valued imports. Approximately \$70 billion was moved out to China via suspect

trade. He then compared those numbers to the overall value of U.S. imports and exports. He found (depending on import or export) approximately 14 to 17% of U.S. trade could well be tainted by customs fraud and perhaps TBML.^{xi}

The above has serious fiscal ramifications. Examining 2021 U.S. trade anomalies, per the above, Dr. Zdanowicz estimates that the U.S. Treasury lost about \$640 billion of taxable profits due to trade-based tax evasion and TBML.^{xiii} The same type of trade fraud revenue loss occurs in every country.

In 2025, China's trade volume was a record high of over \$6 trillion. According to analysis^{xiii} by Global Financial Integrity (GFI), as much as a quarter of China's trade shows signs of potentially fraudulent mis-invoicing. GFI analysis showed that in 2022, the difference between the declared or invoiced value of goods and their actual fair market value totaled a record \$1.7 trillion. Over the past decade, China's invoice value gap was estimated to stand at least \$7 trillion.

GFI reported their findings suggest a "huge hidden leakage" of funds, which could indicate a combination of trade-based money laundering, import tax evasion and capital flight. As noted, GFI analysis indicates 25 percent of Chinese trade is suspect or at least deserves closer scrutiny. So, if we use a very conservative estimate that only 15 percent of trade is suspect, mispriced, or related to forms of trade fraud, that could mean that suspect and possibly illicit Chinese trade is approximately \$900 billion a year and could very easily be much higher than that.

By its volume and sheer dominance of international trade, Chinese actors are assuredly involved with a massive amount of trade fraud. In addition, trade also masks money laundering methodologies and value transfer schemes that are instrumental in a wide variety of SUAs and money laundering methodologies. Generally speaking, trade mis-invoicing and trade-based money laundering are not adequately captured by our current financial intelligence reporting requirements nor are they adequately identified or investigated by Immigration and Customs Enforcement (ICE).

Black Market Exchanges

Although various schemes are used to launder illicit proceeds from the sales of narcotics in the United States, for years the preferred methodology has been the Black-Market Peso Exchange (BMPE). It is arguably the largest and most effective money laundering methodology in the Western Hemisphere. The evolution of the BMPE is an excellent case study of how international criminal networks adapt and how CCP Inc. has incorporated this form of TBML into its business model.

Ironically, the BMPE was not created to launder drug money. In 1967, Colombia enacted regulations that strictly prohibited citizens' access to foreign exchange. Colombian merchants who wanted to import U.S. trade goods – for example, John Deere tractors, Bell helicopters and Marlboro cigarettes – through legitimate banking channels had to pay stiff surcharges above the official exchange rate. To avoid these steep add-on costs, importers often turned to Colombian underground peso brokers, from whom they could buy U.S. dollars on the black market for less than the official exchange rate to finance their legitimate trade.

By the 1980s, the underground peso situation was taking on a new dimension. As U.S. cities found themselves awash in Colombian cocaine, narco-traffickers and cartels were faced with a logistical problem. They had to devise ways to launder and repatriate approximately 20 million pounds of U.S. currency they annually accumulated in North America.

The criminal organizations found a partial solution in the first law of economics. Supply met demand in the form of the BMPE.

Consider a Colombian drug cartel that has sold \$3 million of cocaine in the United States. A representative of the cartel sells these accumulated dollars to a Colombian peso broker at a discount. The cartel is now out of the picture, having successfully sold its drug dollars in the United States and, in return, obtains pesos back in Colombia.

To complete the BMPE cycle, the peso broker must take two more steps. First, he directs his representatives in the United States to “place” the purchased drug dollars into U.S. financial institutions, using a variety of techniques designed to avoid arousing suspicion or triggering financial intelligence reporting.

Second, he takes orders from Colombian businesses for U.S. trade goods, arranging for their purchase using the laundered drug money he owns in the United States. Some businesses should know better, but via “willful blindness,” they don’t ask the questions they should. The broker has laundered the \$3 million in drug money he purchased from the drug cartel.

This money laundering methodology was so successful that the Colombian BMPE became the premier money laundering methodology in the Western Hemisphere in the 1980s, 1990s, and the first decade of the 2000s.

In 2014 there was a turning point. A large law enforcement investigation called Operation Fashion Police showed how Los Angeles–based garment dealers took U.S. drug money and exported their product not to Colombia but to Mexico.

In addition, some of the clothing exporters mixed customs fraud into the BMPE conspiracy. “Made in China” labels were removed from thousands of imported garments. The fraud saved the co-conspirators from paying taxes on the “Made in China” imports because on paper they appeared to be “Made in the USA,” and exempt from customs duties under the North American Free Trade Act (NAFTA).

Once again, with the Mexican BMPE, the proceeds from narcotics trafficking stay on the U.S. side of the border. The same is now true with the cartels’ illicit proceeds in the U.S. from involvement in human trafficking, trade in opioids, kidnapping, stolen cars, weapons smuggling and other illegal activities. Trade goods are purchased and shipped to Mexico. As explained further below, it is a form of “money transfer without money movement.”

About five to ten years ago, the BMPE shifted focus once again. Now, investigators are finding that Chinese manufactured goods are becoming favored instruments in the BMPE and that similar BMPE financial systems are found around the world.

For example, bilateral trade volume between Mexico and China multiplied more than 20 times from 2000 through 2023. In 2024, Mexico’s trade deficit with China reached nearly US \$120 billion.^{xiv} Mexican authorities have said that the surge has allowed drug cartels and their money launderers to piggyback on this burgeoning trade relationship.^{xv} Some of the piggybacking includes TBML, value transfer, and the BMPE.

Fronts for Mexican drug trafficking organizations use illicit proceeds to buy container loads of cheaply made Chinese goods. Using the TBML technique of over-invoicing discussed above, low-quality Chinese manufactured items are made to appear on paper as being worth significantly more. Payment for the goods is sent out of the country. That's the wash.

We see the result of this in our cities and communities in America and around the world, but we don't recognize or understand what is going on. Massive quantities of cheaply manufactured Chinese goods including counterfeits are found in black markets as well as souks, bazaars, marketplaces, dollar stores, Mom and Pop shops, swap meets, street kiosks, "China shops," and warehouse stores around the world.

In some cases, brokers under-invoice Chinese products. A variety of goods including electronics, garments, small household appliances, are purchased, imported, and sold in many "China shops" and on the black market in countries around the world. Via this form of value transfer, funds are used to buy contraband including drugs, ivory, endangered and illegal wildlife and their parts, and heavily regulated flora and food items that are later shipped to China. This is why I noted earlier in my testimony that the CCP business model and its involvement with various SUAs are intertwined and cannot be examined in isolation.

The BMPE has evolved further still as Mexican and other foreign national buyers and brokers travel directly to China to place orders for the goods or they avail themselves of e-commerce brokers to purchase consumer products that are made in China. Generally speaking, Chinese merchants also practice willful blindness. They do not conduct customer due diligence and do not care if they are being paid with illicit proceeds.

Capital Flight

Capital flight is not considered money laundering. However, it can be in some circumstances. If the capital that is fleeing is "mixed" or "co-mingled" with dirty funds that are the result of SUAs then by common law enforcement characterization all of the money is tainted. In addition, many of the methodologies used by those that practice capital flight are identical to those used to launder money. Capital flight can also involve the three recognized stages of money laundering: placement, layering, and integration.

China leads the world in capital flight. An estimated \$1 trillion in capital flowed out of China in 2025, the largest annual outflow since records began in 2006. Due to the hemorrhage, the CCP is tightening capital controls. In addition, China's State Administration of Foreign Exchange (SAFE)—a government agency under the Peoples Bank of China (Central Bank), stipulates that in most circumstances the maximum value of foreign exchange transactions permissible by a Chinese citizen in a calendar year is the equivalent of U.S. \$50,000.

So, Chinese citizens who wish to transfer funds—licit or illicit—out of the country outside of the watchful eyes of SAFE must find other means to do so. This testimony summarizes some money laundering methods in the transfers including trade-based value transfer, black market exchanges, flying money, and mirror accounts or “swaps” (see below) that, via a broker, exchange illicit funds in the United States for Chinese capital.

Few question the negative effects of Chinese capital flight and its possible links to money laundering. We should. As David Mulroney, the former Canadian Ambassador to Beijing, succinctly said, “China is the number one exporter of hot money to the world.”^{xvi} Another way of describing “hot money” is “proceeds of crime.”

Particularly troublesome is Chinese capital that is invested in U.S. real estate including farmland in strategic locations and the purchase of American homes. Chinese are the largest percentage of foreign homebuyers. In 2025 alone, Chinese spent \$13.7 billion on American homes. More than two-thirds of Chinese buyers (71%) made an all-cash purchase.^{xvii}

In 2025, FinCEN reported that Chinese Money Laundering Networks (CMLNs) are using criminal proceeds within the U.S. to purchase high-value real estate. These networks facilitate a "swap" that benefits both transnational drug cartels and wealthy Chinese nationals looking to bypass the strict domestic capital controls described above.^{xviii} Money or value is transferred, but stays in place. This makes it more difficult for law enforcement to follow the money trail.

In my opinion, some American professionals such as attorneys, accountants, and real estate agents facilitate these and other transactions by willful blindness and lobbying strenuously to be exempt from BSA reporting requirements.

Also troubling, many Chinese buyers use their new home as a way to gain permanent residence in the United States, giving them preferential access to things like a college education

for their children. The purchases worsen the housing shortages for Americans citizens and also price Americans out of desirable housing markets.

Mirror Swaps

Over the past five years, Chinese money laundering rings have been increasingly moving the drug proceeds of the Mexican cartels. Since China's financial regulators limit private individuals from handling more than \$50,000 in foreign currency, there is massive Chinese demand for U.S. dollars. This pent-up demand for dollars from China and the cartels' need to unload U.S. dollar proceeds creates this unholy alliance between Chinese money launderers and the Mexican cartels. They engage in a broad spectrum of mechanisms to move and obfuscate the origins of drug proceeds such as bulk cash smuggling, trade-based money laundering, mirror swaps, cryptocurrencies, and digital payment platforms like WeChat Pay and Alipay, shell companies and real estate.

Chinese actors working with the Mexican cartels have pioneered the growing use of "mirror accounts" or "mirror swaps" to launder the proceeds of crime.

With "swaps," Chinese brokers often working with Chinese organized crime groups and the cartels identify Chinese/American cash intensive businesses that are willing to cooperate. They often use Chinese social media apps.

How do the swaps work? The Chinese/American businessperson receives the drug cash from the Chinese broker working with the cartels. The business later "places" the proceeds of crime into its revenue flow and represents the drug cash as legitimate proceeds from the business. Or, the cash is used to assist other Chinese that want to circumvent Chinese capital flight restrictions and, for example, purchase U.S. property, housing or other high-ticket goods.

Meanwhile, these complicit businesses are asked to transfer a designated amount of money through Chinese phone apps to accounts based in China. Using a currency converter app on a smartphone, the participants agree on the exchange rate between the U.S. dollar and the Chinese yuan. Once the money is offshore in China, the value can be further re-routed to Mexico or elsewhere per the instructions of the cartels.

It's called a “swap” because the participating businessperson takes possession of the drug cash, while simultaneously transferring the equivalent in Chinese yuan from his/her account in China to the account provided by the broker. Of course, the Chinese/American businessperson also receives a commission.

During the original Colombian BMPE, the average commission for the black-market peso broker was about 15%. The Chinese are doing it for 1 to 2% on average.^{xix} And the speed is almost instantaneous. For the traffickers, the big plus is that the Chinese organized crime groups involved absorb all the risk. The cartels know they will get paid.

Communications are generally accomplished via Chinese apps such as WeChat. Law enforcement is reportedly challenged to monitor the communications and monetary transactions. Yet the same transactions are easily monitored by the platforms involved as well as Chinese intelligence entities. Mirror swaps also avoid U.S. financial intelligence reporting requirements – our primary anti-money laundering countermeasure.

Fei-Chien or Flying Money

Chinese underground finance or alternative remittance systems are primarily used to remit wages from the Chinese diaspora back to the homeland. Authorities have no wish to interfere with hard-working immigrants sending money “back to the home country” to help support extended family in China. Most of these money transfers are perfectly benign. Unfortunately, these low-cost and highly efficient financial systems are also abused by criminals to move, transfer, and launder illicit proceeds. Increasingly, the transfers are multi-directional. The system is very attractive to criminals because by its very nature it is opaque. Generally speaking, U.S. law enforcement does not understand or recognize Chinese underground finance. There are few trails for authorities to follow. Chinese underground finance or alternative remittance systems also avoid government scrutiny, taxes, and traditional countermeasures such as the filing of financial intelligence reports.

It is believed that *fei-chien*, sometimes known as “flying money,” was started during the T’ang Dynasty (618 to 907 AD).^{xx} At the time, there was a growing commodity trade within China. Some historians believe it was the rice trade and others the tea trade that were the catalysts for this new financial system. Ironically, as opposed to modern day practices, the

transfer schemes were not invented as underground methods of payment transfers, but were rather systems devised by the government to facilitate taxation. Merchants sold their goods and then brought their revenues to provincial “memorial offering courts.” The government collected taxes. In turn, the merchants were issued certificates for the remaining value of the commodity sales. When the merchants returned to their home provinces, they would present the certificates to the provincial government for payment. Interestingly, some scholars believe these certificates were the forerunner of the paper banknotes that appeared during the Song dynasty (960 – 1279 AD). The *fei-chien* system became an efficient way of payment. Completing transactions in this way spared both the merchants and government the risk of transporting large sums of money and ensured all parties would get paid.

Over the centuries, the *fei-chien* system continued to evolve. Chinese workers increasingly began to migrate to remote provinces, and then overseas. The Silk Road trade between China, Central Asia, and Europe created a demand for brokers at the ends of the major trade routes who were prepared to settle each other’s debts. Negating the need for physical currency or gold to travel was an important security consideration. In addition, families back home needed financial support to maintain their livelihoods. Expatriate Chinese businesses began to develop side businesses of remitting money back to China. The international Chinese diaspora spread this indigenous financial system further still. Today, modern Chinese businesses as well as “Chinatowns” and “China shops” and Chinese organized criminal groups are found around the world. So too is Chinese flying money. Chinese underground banks are a new iteration of an age-old financial system, re-purposing informal value transfer techniques for today’s world.

Strong Chinese family bonds are incorporated into “*guanxi*,” which is an overarching social system of rules that govern relationships and social behavior. *Guanxi* is the guarantor of both secrecy and the integrity of the parties to the transaction. Those who violate its prescriptions find themselves as social outcasts, essentially shunned in all circles. *Guanxi* is an integral component of *fei-chien*. In other words, similar to hawala and other better known indigenous informal value transfer systems, an essential element is trust. The trust is based on family, clan, social mores, friendship, and culture. As a result, it is very difficult for outsiders to penetrate the *fei-chien* underground financial networks.

Let's use a simple scenario to illustrate how Chinese flying money works: Wang in Guangdong province wants to send 200,000 Chinese renminbi (RMB) to his brother in New York City. Wang wants to protect his hard-earned money by investing in dollars and the United States. He uses a series of underground flying money transfers to avoid the PRC's tight capital restrictions. Wang gives the Guangdong "flying money" broker the RMB and in turn receives a code number. He trusts the broker as they have a familial relationship. The "flying money" broker in Guangdong directs his counterpart in New York (perhaps a member of the same family) to pay the equivalent in U.S. dollars (approximately \$29,500) upon presentation of the code. The code could be transferred in a telephone call or a message contained in an e-mail or perhaps the Chinese messaging system, WeChat. Not many years ago, a playing card or a portion of a currency note with a specific chop, marking, wax seal, or other physical sign would be presented to the broker as a sign of authentication. If it is a recurring transaction, codes aren't necessary. Upon receipt, the New York "flying money" broker pays Wang's brother in New York City. The RMB did not physically leave China. The dollars were already in the U.S. Similar to hawala, the system can be described as "money transfer without money movement."^{xxi} Wang's brother safeguards the \$29,500 and following transfers. His brother's capital is now in the United States and authorities are none the wiser.

Money and value are also sent back to China. Like all immigrant groups, Chinese send money back home to help support their families. The same fei-chein brokers are involved. Even though "flying money" largely operates on trust and community ties, the brokers are in business to make money. Occasionally they have to settle accounts. Transactions are multi-directional. Using the above example, the New York broker might be running a deficit or a surplus with his counterpart in Guangdong. Various methods are used to settle accounts including banks, cash couriers, online payment services, mirror accounts, and trade-based value transfer.

Surplus credits could also be used by a client unrelated to the original transaction(s). For example, as explained above, credits could be used for the purchase of foreign real estate. For a fee, the client that wants money outside China pays RMB in China to a flying money broker and receives credit in the desired foreign location in local currency.

One of the most popular methods of getting RMB or yuan out of China involves finding a willing foreign contact who would like to set up a private exchange for Chinese RMB. Flying

money networks are sometimes used but so are informal personal networks and business associates. For instance, the overseas person puts their dollars into an account in Hong Kong or Singapore belonging to the Chinese individual. The Chinese individual in China puts the Chinese RMB in an account in Beijing that is connected with the overseas investor who wants the money in China.

What is often overlooked in hawala, flying money, and other informal underground financial systems is that historically and culturally *trade is most often used in the settling of accounts between brokers*. Per the above discussion of trade fraud, value transfer, TBML and fraudulent invoicing, value transfer or “counter-valuation” has been used as an efficient and effective settlement system for thousands of years. Most “flying money” brokers are directly involved or associated with trading companies - especially now that China is a global economic and trade power.

How do the “flying money” brokers profit? Although commissions are paid to the brokers at both ends of the transaction, the fees are less than banks or traditional money remitters such as Western Union charge. In comparison to large brick-and-mortar banks and money transfer chains, expenses are small. Often the brokers use legitimate businesses as fronts. The businesses include restaurants, China shops, and trading companies. Of course, in the underground remittance segment of their business they skirt regulations and taxes. In the United States, the flying money brokers are technically classified as a money service business (MSBs) for the purposes of registration, licensing, and reporting financial intelligence. They must register with FinCEN and be licensed in 48 of the 50 states. They are also supposed to file financial intelligence. They do not comply.

After the September 11 attacks in the United States, law enforcement and intelligence agencies began to focus on hawala and its links with terror finance. As a result, hawala has received much worldwide attention and notoriety. There have been a number of successful investigations into how hawala is misused by criminals and terrorists. Because of the worldwide Chinese diaspora, I believe the magnitude of “flying money” is larger than hawala. Together, underground remittance systems could be valued at over \$1 trillion per year.^{xxii} The important point to note is that both of these culturally-based systems are efficient and historically and culturally rely on trade-based value transfer.

I have the utmost admiration and respect for these underground financial systems. They are fast, efficient, reliable, functional, and provide much needed low-cost financial and remittance services for millions of people around the world. The primary drawback, of course, is that criminals take advantage of the systems' opacity and anonymity. Flying money is used to launder the proceeds of crime. These "underground," "parallel," or "alternative remittance systems" are very difficult for law enforcement and intelligence services to monitor. Most law enforcement at the federal, state, and local levels are not even aware of the existence of flying money. There are very few investigations.

Chinese Students in U.S. Doubling as Money Launderers

The estimates vary, but there are approximately 300,000 – 500,000 Chinese students in the United States. Unfortunately, there are reports that Chinese students in the U.S. are increasingly recruited by CMLNs to act as "money mules." Students are often targeted by Chinese money brokers due to financial pressures or a lack of awareness regarding the illegality of their actions. CMLNs use social media, messaging apps (like WeChat or Telegram), and personal networks to find participants. Students may be told they are simply providing "money transmission services" for other international students or helping unbanked Chinese citizens. Recruitment is also driven by willful blindness, cash fees, cultural obligations, intelligence operatives (see below), and "debt bondage."

According to FinCEN, from 2020-2024, financial institutions in the U.S. filed 20,282 BSA reports totaling almost \$14 billion in suspicious activity that referenced individuals purporting to be Chinese students.^{xxiii} According to FinCEN's analysis, many transactions involved U.S.-based Chinese nationals depositing large amounts of cash disproportionate to their income. These funds were often immediately transferred to other accounts or converted to cashier's checks, which FinCEN linked to Chinese citizens' efforts to expatriate funds past China's strict currency control laws described above. FinCEN found that CMLNs frequently collaborate with transnational criminal organizations, such as Mexico-based drug cartels, to launder and move illicit proceeds through the U.S. financial system.

Chinese students are also involved with "daigou" and gift card fraud.

Daigou

Over the years, Australian and U.K. law enforcement have reported a surge of fraud and money laundering related to *daigou* or “buying on behalf of.” Although seldom recognized in the United States, it is definitely here. Daigou exists because Chinese consumers crave quality Western products that are in short supply and routinely subject to high taxes in China. As a result, surrogate shoppers in western countries purchase goods and ship them to China directly or route them through intermediary countries via specialized logistics brokers taking advantage of duty-free pricing, favorable exchange rates and specialized routing to help circumvent customs and taxation. Some organized daigou networks use travelers' "personal use" exemptions to enter goods into China.

Daigou networks generally operate by advertising luxury products on Chinese e-commerce sites or social media platforms like WeChat or TaoBao. Common daigou products include high-end designer bags, apparel, and watches from brands like Chanel, Louis Vuitton, or Gucci; premium beauty products from companies such as La Mer, Estée Lauder, or SK-II; vitamins and wellness products and quality infant baby formula and food; and Apple I-phones and high-end western electronics.

Investigations show that some of the daigou networks operate with CMLNs. Cartel and drug money are used to recruit daigou "mules" (often Chinese students in the U.S.) who purchase high-value electronics and luxury goods. These items are then exported to China and sold, effectively washing the illegal cash through legitimate international retail channels.

In Operation Take Back America, members of a professional daigou network pleaded guilty to laundering over \$92 million. The scheme utilized thousands of individual shoppers who were recruited to use illicit cash to buy luxury items across the United States. The items were consolidated and exported to hubs in Asia.^{xxiv} Daigou networks in the U.S. can falsify customs forms or commercial invoices, thereby undervaluing shipments described above in the section on trade-based money laundering.

Gift Card Theft and Scams

Many of the daigou products procured in the U.S. are stolen or otherwise fraudulently obtained by a CMLO. For example, there are investigations into CMLOs involved in large retail gift card fraud schemes that involve removing, altering, then re-stocking gift cards at retail stores. During the alteration process, the gift card barcodes are replaced by barcodes controlled by the CMLO. When the unwitting customer loads funds onto the altered gift card, the CMLO uses the phones to purchase goods, often iPhones and other daigou related products, through retail purchases made by CMLO mules throughout the United States. The iPhones, together with other goods purchased with criminal proceeds, are then exported abroad for resale to complete the Chinese underground banking cycle.^{xxv}

Proceeds are also sometimes converted into digital currency and funneled back through Chinese payment platforms to disguise the source of the funds. The same platforms are used in “mirror swaps” described above. In addition, offshore Chinese owned and operated telemarketing and e-commerce scam groups trick individuals via phone, texting, or online into purchasing gift cards and sharing the redemption codes. The scams sometimes use artificial intelligence to target suspects. The Chinese organized crime groups also use AI voice cloning to target Americans, many elderly, through scams that involve impersonation of authority figures or loved ones in distress. Payment is demanded in gift cards or cyber currency. The criminal organization sends the gift card information to colleagues in the United States to purchase consumer goods, which are then shipped to China and other locations for resale at significant profits.

Intelligence Operatives

The CCP is intent on leveraging a worldwide network of covert agents to monitor and influence events outside its own borders, steal vital assets and technology, and to surveil and intimidate Chinese dissidents in America and elsewhere. China's Ministry of State Security (MSS)—China's primary foreign intelligence agency—employs up to 600,000 people globally. There are estimates that tens of thousands of Chinese intelligence officers operate in the U.S. And unlike compartmentalized Western intelligence agencies, China relies on a broad and diverse network including not just professional case officers, but also scientists, academics,

corporate insiders, and private citizens to gather civilian, commercial, military technology, and engage in “elite capture” and influence operations.

Chinese civilian intelligence services operate under the guidance and direction of the CCP. Further, there is an undefined symbiotic and malevolent relationship between Chinese intelligence services and Chinese organized crime. Though not a chain of command, overseas Chinese intelligence agencies and Chinese organized crime maintain a pragmatic, mutually beneficial bond. Beijing selectively uses these criminal networks as proxies. In addition, Chinese state intelligence operates under the broader United Front system, which views any overseas Chinese individual, group, business, or non-state entity as a tool to promote CCP interests abroad.

China’s National Intelligence Law from 2017 requires organizations and citizens, wherever they are in the world, to “support, assist and cooperate with the state intelligence work.” It gives the appropriate Chinese authorities the power to monitor and investigate foreign and domestic individuals and institutions. As part of this law, Chinese intelligence agencies can search premises, seize property, and mobilize individuals or organizations to carry out espionage. The law also gives intelligence agencies legal ground to carry out their work both in and outside China.^{xxvi}

The 2017 National Intelligence Law can easily be used to facilitate many of the SUAs and money laundering methodologies discussed above. For example, a Chinese person living overseas—a citizen of the PRC or not—can be simply ordered by the appropriate Chinese intelligence service to let their bank account be used in the layering process of money laundering; a hard working Chinese citizen’s overseas business might be co-opted to serve as a front for nefarious purposes; a Chinese-owned business might be used to import or export contraband; a well-placed Chinese businessman or academic can be easily pressured to reveal any manner of information deemed of import; a promising overseas Chinese student or young professional might be directed against his or her will into a position that provides access to desired information or to engage in money laundering.

In other words, the National Intelligence Law is not about traditional intelligence collection. There is no “tradecraft” involved. It is a blanket mandate from an authoritarian

command state that demands servile obedience to the demands of intelligence organs working for the CCP in order to fulfill China's national interests. This is a huge, but largely unrecognized, factor in fighting both Chinese criminal activity and protecting our national security.

Recommendations

CCP Inc.'s criminal activities are increasingly exposed. I believe CCP Inc. is very vulnerable to a systematic and coordinated law enforcement approach. The following suggestions are offered in no particular order or priority. Most of them focus on law enforcement and related topics. I have made recommendations for combatting individual SUAs and money laundering methodologies elsewhere.^{xxvii}

Develop a U.S. Law Enforcement Strategic Plan Focused on CCP Inc. Crime

Although there have been sporadic plans to counter China, none has focused on the *totality* of CCP Inc criminality and money laundering. An effective strategic plan should not fall under the purview of one government department or bureau. Much of the criminality and financial crimes described is beyond the scope and expertise of the FBI alone. CCP Inc. criminality is extensive and wide ranging. There are multiple SUAs that demand attention. Crimes, Chinese-centric money laundering methodologies, and the threats posed by Chinese organized crime and intelligence services within the United States should be looked at as parts of a whole. The China threat in the U.S. should be treated as an on-going criminal enterprise. These transnational crimes cut across the mandates of several U.S. intelligence, law enforcement, and regulatory agencies. The Department of State needs to become engaged. State and local police have roles to play. We need an all-encompassing plan of action.

Establish CCP Inc. Task Forces

The U.S. government has constructed several specific federal task forces and strike forces to target Chinese transnational organized crime. But they are segmented and concentrate on one particular type of violation of law or threat. As noted, we need to focus on the *totality*.

Over the last decades, U.S. law enforcement has enjoyed considerable success establishing task forces comprised of federal, state, and local law enforcement. There may be

concurrent jurisdiction when, all at the same time, a crime is a violation of federal, state, and local law enforcement. Task forces typically focus on terrorism, organized crime, narcotics, gangs, and human trafficking. Some of the best-known national task forces are the Organized Crime Drug Enforcement Task Forces (OCDETF) and the Joint Terrorism Task Forces (JTTFs). The Director of National Intelligence and other U.S. intelligence agencies often assist the task forces in gathering and analyzing intelligence related to national security threats.

I propose establishing new task forces comprised of federal, state, and local law enforcement that specifically target the CCP Inc. threat domestically. And, understanding and adhering to the constraints posed by venue and jurisdiction, investigate the Chinese criminal presence overseas. This must be done in concert with our partners. Foreign investigations should include Chinese triads' involvement in illicit trade in ports, FTZs, Belt and Road Initiative projects, transnational crime of all sorts, cross-border money laundering operations, and corruption. Certain CCP Inc.-backed crimes are currently being investigated, such as espionage and intellectual property theft. But, once again, we need an understanding of the interconnectedness of the threat including the relationships between criminal networks and their enablers engaged in a variety of SUAs. We need to focus on uniquely Chinese ways of laundering money and transferring value. We have to better understand the relationship between the government of China, its intelligence services, and organized crime. An isolated FBI field office or even a task force dedicated, for example, solely to narcotics trafficking is not going to be able to do that.

Multiple regional China Inc. task forces should receive specialized training. They should be directed by Assistant U.S. Attorneys that have an aggressive approach but fully adhere to the law and respect and safeguard civil liberties.

Really, Truly, Finally Go After the Money

U.S. law enforcement has consistently talked about the importance of “following the money” and taking away the proceeds of crime from criminals and criminal organizations. Yet in practice those self-evident goals have not been emphasized. To take just one notorious example, in our “War on Drugs” our efforts have been concentrated on interdicting the participants and the products. Another strategy the DEA and other law enforcement organizations pursue is to go

after the “kingpins” or the leaders or heads of criminal organizations. The strategy is to decapitate the boss of bosses and kill the organization. A further tactic is to go after the low-level participants—the street-level dealers and the mules and follow them to the top of the organizational structure. However, the most common counter measure of all is to go after the product, from bags of fentanyl and opioid products smuggled across the border to tons of cocaine seized on the high seas. The history of the drug wars over the last 30 years has shown that none of these tactics have been effective.

Having been in federal law enforcement, I’ll tell you the truth: we go after the participants and the product because it is far easier than going after the money. Also, the product is not just drugs. It similarly holds true for human beings in trafficking networks, counterfeit goods, illicit tobacco, wildlife trafficking, etc. All of the above and many more are SUAs for CCP Inc. money laundering. Criminals do not traffic in drugs for the sake of drugs or any other illegal good or service. They engage in crime for the money. Following the money trail and taking away proceeds of crime will hurt the criminal organization far more than a prison term or a seizure of contraband. Our emphasis on product and participants has led to failure. But the law enforcement bureaucracies persist in their efforts primarily because of careerism, bureaucratic culture, and lack of imagination. Law enforcement is “stat” driven because that is how individuals, offices and departments, bureaus and agencies are recognized. More stats generally mean larger budgets. To this end, it is far easier and more productive from a bureaucratic perspective to go after people and products than money. Quick and easy but non-consequential “busts” are far easier for bureaucracies than to engage in a long-term complex money laundering investigation. But these often lengthy and multifaceted cases historically are the ones that make a real impact. In order to change that paradigm, we must target and finally prioritize the proceeds of crime. To make that happen, we have to change the incentives and the culture of the law enforcement bureaucracies. I have written about this important topic elsewhere.^{xxviii}

Put Customs Back into the Department of Treasury Where it Belongs

In the rush to react to the events surrounding September 11, politicians of both parties hurried to create the new Department of Homeland Security. The multiple problems of DHS have been chronicled elsewhere. But few discuss how the merger of Customs and the old

Immigration and Naturalization Service (INS) into Immigration and Customs Enforcement (ICE) has negatively impacted our AML efforts.

The U.S. Customs Service was originally created on July 31, 1789, when the Fifth Act of the First U.S. Congress was signed into law to collect duties on imported goods. Logically, it was part of the Department of Treasury. In modern times, Customs Office of Enforcement evolved. Customs Special Agents carried badges, guns, had the power of arrest and conducted investigations. They had jurisdiction on most crimes dealing with the border. In fact, legacy Customs enforced more laws than the FBI. Importantly, because Treasury was its home, almost by definition Customs enforcement concentrated on money and value – particularly as it relates to trade. In the 1980s and 1990s, almost all of the large, impactful, meaningful, trend setting, anti-money laundering investigations were initiated by Customs. The forced integration into DHS changed all of that.

Over the last 23 years, the primary mission of ICE has been immigration. Resources, manpower, expertise, and political capital have been diverted from traditional customs issues and into immigration enforcement. Meanwhile, legacy customs' jurisdictions suffered by neglect. Priorities shifted. Expertise departed. Upper management shifted funds meant for customs to immigration. Most ICE Special Agents today are woefully lacking in AML and customs fraud expertise. Particularly in dealing with trade-based money laundering and value transfer, the FBI and other federal law enforcement agencies are not capable of taking up the slack. They don't have the data, proficiency, or mandate.

In my opinion, the single best thing this Congress could do to meaningfully combat our primary anti-money laundering failure – the lack of effective enforcement, is to right a historic wrong and put U.S. Customs back into the Department of Treasury where it belongs. Beef up traditional customs enforcement. Not only will it drastically help solve many of the enforcement challenges outlined in this hearing, but increased customs enforcement will also add to the general revenue via enhanced fines, penalties, seizures and forfeitures.

And while Congress is at it, I strongly suggest that the once proud and respected U.S. Secret Service also be taken from DHS and returned to the Department of Treasury where it historically belongs and its culture more closely aligns.

Law Enforcement Needs Beneficial Ownership Information

Over the last 50 years, there have been a plethora of AML legislation designed to help financial crimes investigators. In my opinion, the last significant missing piece of legislation is the lack of meaningful beneficial ownership information on various LLCs, front, and shell companies. Shell companies are formed under U.S. state law, by registered agents, to obscure the identities of those who benefit from and control them. It is extremely frustrating for federal, state and local law enforcement, as well as many of our foreign law enforcement counterparts, to follow hidden money and value trails to offshore shell company accounts only to find the beneficial ownership and/or true account registration information is simply not available.

Treasury's FinCEN reported that financial institutions reported over \$312 billion in suspicious activity tied to decentralized, horizontal Chinese CMLOs operating as a service for Mexican cartels like Sinaloa and Cartel Jalisco Nueva Generación (CJNG). These networks heavily rely on networks of US-registered front and shell companies. ^{xxix}

I understand that implementing the Corporate Transparency Act (CTA) is now stalled and U.S.-formed companies and U.S. citizens are now exempt from beneficial ownership information reporting requirements. Others can debate the efficacy of the CTA legislation, the unintended reporting burdens, or if FinCEN has demonstrated the ability to effectively manage yet one more database. (The record shows that FinCEN has been historically challenged in fulfilling its mission. Yet it is mandated with ever increasing responsibilities). But regardless of how the CTA debate is settled, I strongly urge that we continue to work towards collecting targeted shell company beneficial ownership information. Law enforcement and appropriate regulators should have efficient access to the data in order to truly follow hidden money and value trails and better safeguard our financial system.

Enablers Should be Subject to Mandatory BSA Reporting Requirements

Criminals and criminal organizations rely on professionals who provide advice and financial services to facilitate the three stages of money laundering – placement, layering, and integration. In other words, many times professionals are vital in creating non-transparent distance between the real owner and the suspect funds. Since the enactment of the USA Patriot

Act, lawyers, accountants, and real estate professionals have been inconsistently covered under mandated BSA reporting requirements.

The FATF's international standards (specifically Recommendation 22) require countries apply AML obligations to Designated Non-Financial Businesses and Professions (DNFBPs). In its latest mutual evaluation or comprehensive review of the U.S., FATF cited this lack of coverage as a critical vulnerability. Because lawyers and other professionals act as gatekeepers who form shell companies and facilitate transactions, the lack of due diligence and suspicious activity reporting leaves the U.S. financial system open to exploitation. And, for example, investment in U.S. real estate remains one of the primary methods of choice criminals and criminal organizations use to launder illicit proceeds.

The U.S. has consistently resisted or delayed bringing these professional enablers under mandatory BSA reporting regulatory umbrella. No doubt this longstanding situation is due to the fact that all of the above professions and business interests expend significant amounts of money in influential lobbying operations. The American people pay the price. The situation is shameful and should end. Mandatory BSA reporting for professional enablers, combined with beefed up SAR analysis at FinCEN and enhanced enforcement in the field, are vital to successfully pursue and prosecute the broader networks that power and protect illicit finance.

Enforce the Obligation of Informal Money Remittance Dealers to Register as Money Service Businesses

CCP Inc.-based money remitting applications operating in the United States (that are also involved in money laundering), are required to register as money services businesses (MSBs). Some have not registered. Moreover, only a tiny fraction of informal money remitters such as hawaladars and fei-chien brokers have actually registered with Treasury's FinCEN or, as mandated, report suspicious activity.

Formulate Intelligence Collection Taskings

I am out of the U.S. intelligence and law enforcement communities now, but it appears the concerned bureaus, agencies, and departments are for the most part ignorant about the totality of CCP Inc. transnational crime and, in particular, money laundering methodologies. This will only change when policymakers make it a matter of import. I urge the President of the United States to take action.

John A. Cassara
www.JohnCassara.com

States to task the Office of Director for National Intelligence to include in the National Intelligence Priorities Framework (NIPF), and through Intelligence Community directives, to have the Central Intelligence Agency (CIA), National Security Agency (NSA) and other applicable intelligence agencies develop intelligence reporting requirements for HUMINT and SIGINT and other collection means that target Chinese transnational crime and money laundering globally. I further urge the release of unclassified overlays of global illicit markets with significant Chinese corruption and criminality (e.g., BRI). Within classification guidelines, criminal investigators should be given access to the finished intelligence products to assist them in their targeting and investigations.

The FATF Should Name and Shame China

In the world of anti-money laundering/counter-terrorist financing (AM/CFT), it is the Financial Action Task Force (FATF) that makes things happen.

The FATF was created in 1989 by the G-7 to combat international money laundering. The FATF is an international AML/CFT policy making body. It does so primarily through its 40 recommendations and periodic mutual evaluations that ensure countries adhere to the internationally accepted AML/CFT guidelines. I have been directly involved with the FATF in its annual plenary meetings and the mutual evaluation process serving as a law enforcement “expert.” While the FATF, and FATF-style regional bodies, have done much good and have been highly successful in bringing attention to the scourge of international money laundering, the FATF has simply not fulfilled its original mission—curtailing international money laundering. What is not openly discussed is that by the “metrics that matter,” i.e., money laundering convictions and asset forfeiture, over the last 30 years our efforts have been disappointing. As I quoted in the beginning of this testimony, “Total failure is just a decimal point away.”^{xxx} Money laundering enforcement has failed both in the U.S. and around the world. The reasons are many and I have written about them elsewhere.^{xxxi}

Internationally, one reason for failure is that the FATF 40 Recommendations and mutual evaluation process have evolved into a procedural box checking exercise. The boxes reflect debate about whether or not a country is “compliant” with a recommendation/s. What’s lost in the discussion is the original founding intent of the FATF and the effectiveness of AML/CFT as

measured by the metrics that matter. Moreover, countries are afraid of being put on the FATF “blacklist” (something that doesn’t really exist) because of bad publicity and international risk, ratings and credit concerns. So, in response to FATF pressure, countries often pass legislation or create rules or make promises to get the FATF off their back. This is all well and good.

Unfortunately, I have seen in my career that after the evaluation process and the checking of boxes some countries soon go back to business as usual. Countries posture and make promises. However, they don’t have the political will to use their own initiative and truly combat AML/CFT. In the arena of combating international money laundering, we are only as successful as the weakest link. The Peoples Republic of China is a classic example of a very weak link. There are others.

In the most recent 2019 FATF mutual evaluation of China, none of the issues raised in this testimony were addressed. In my opinion, the mutual evaluation was simply another box checking exercise with political overtones if not unspoken pressure (China held the presidency of the FATF during the evaluation process) that did nothing to confront CCP Inc.’s involvement with transnational SUAs and money laundering.

As I state in my book *China – Specified Unlawful Activities*, measured by SUAs and China-centric money laundering methodologies and enablers, CCP Inc. represents the greatest money laundering threat in the world. Thus, despite China’s latest mutual evaluation report, I urge the U.S. FATF delegation to build consensus within FATF to “name and shame” China. Other like-minded delegations should join the call. The same should happen in the FATF-style regional bodies of which China is a member – the Asia Pacific Group and the Eurasian Group on Money Laundering.

The FATF Should Create a New Recommendation that Specifically Addresses TBML

I have written about this elsewhere,^{xxxii} and have also addressed it in previous Congressional testimony, but the international community will never seriously make progress against trade-based money laundering (TBML) and associated crimes such as black-market exchanges and flying money unless and until the FATF creates a new recommendation that specifically addresses the issue.^{xxxiii} Trade fraud is a very significant SUA for money laundering. Depending on its varied forms, TBML can also act as a money laundering technique or

methodology. I believe it is the largest and most prevalent of all the money laundering methodologies. Moreover, trade fraud and TBML are inextricably intertwined with many of the CCP Inc. criminal activities and money laundering discussed. It has become part of CCP Inc.'s business model. It is time the FATF addressed the issue and create a specific anti-TBML recommendation. The U.S. delegation to the FATF should be directed to make this happen.

References

- ⁱ Ron Pol cited in: Hamish Fletcher, "Dirty cash: The fight against money laundering - should NZ do more?" The New Zealand Herald, September 10, 2015. (http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11510931)
- ⁱⁱ United Nations Office on Drugs and Crime, "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, United Nations Office on Drugs and Crime," October 2011; https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
- ⁱⁱⁱ Raymond Baker, *Capitalism's Achilles Heel*, (Hoboken, New Jersey: Wiley & Sons Publishing, 2005), page 173.
- ^{iv} "Money laundering costs \$5.5 trillion USD across the globe, Napier AI finds," October 21, 2025; <https://www.napier.ai/post/ai-aml-index-2025-2026>
- ^v Joseph Ibitola, "Overcoming the Hidden Costs of AML Compliance," Flagright, June 30, 2025; <https://www.flagright.com/post/overcoming-the-hidden-costs-of-aml-compliance>
- ^{vi} Channing Mavrellis, "Transnational Crime and the Developing World," Global Financial Integrity, March 27, 2017; <https://gfindtegrity.org/report/transnational-crime-and-the-developing-world/>
- ^{vii} Note: Full disclosure – I am proud to be on the Board of Directors of GFI.
- ^{viii} For details, see John Cassara and David Luna, "Criminals Accelerating Global Illicit Trade by Exploiting Digital Assets, Trade Finance Fraud, and other Emerging Transaction Laundering Schemes," International Coalition Against Illicit Economies (ICAIE), April, 2026; <https://icaie.com/2026/03/criminals-accelerating-global-illicit-trade-by-exploiting-digital-assets-trade-finance-fraud-and-other-emerging-transaction-laundering-schemes/>
- ^{ix} "Members of Transnational Money Laundering Organization Charged with Laundering Cartel Funds," Department of Justice Press Release, May 22, 2026; <https://www.justice.gov/opa/pr/members-transnational-money-laundering-organization-charged-laundering-cartel-funds>
- ^x "Trade Based Money Laundering," the FATF, Paris, June 23, 2006, p. 1; <http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf>
- ^{xi} Data and analysis were given to the author by Dr. John Zdanowicz
- ^{xii} "U.S. Tax Cooffers Lose \$640 billion of Taxable Profits due to TBML Evasion and Money Laundering in 2021," SEK Strategies, May 4, 2022; <https://www.prnewswire.com/news-releases/us-tax-cooffers-lose-640-billion-of-taxable-profits-due-to-trade-based-tax-evasion-and-money-laundering-in-2021-says-sk-strategies-301539461.html>
- ^{xiii} "Trade-related Illicit Financial Flows in Developing Asia, 2013–2022," Global Financial Integrity, March, 2026; <https://gfindtegrity.org/wp-content/uploads/2026/03/Trade-IFFs-in-Asia-Final-Final-March-25.pdf>
- ^{xiv} "Mexico's half-year trade deficit with China hits a record US \$57 billion," Mexico News Daily, August 14, 2025; <https://mexiconewsdaily.com/business/mexicos-trade-deficit-with-china/#:~:text=Bilateral%20trade%20volume%20multiplied%20more,reached%20nearly%20US%20%24120%20billi on.>
- ^{xv} Drazen Jorgic, "Special Report: Burner phones and banking apps: Meet the Chinese 'brokers' laundering Mexican drug money," Reuters, December 3, 2020; <https://www.reuters.com/article/us-mexico-china-cartels-specialreport-idUSKBN28D1M4>
- ^{xvi} Frank O'Brien, "Property sales spike sparks money laundering fear," Compliance Alert; <http://www.calert.info/details.php?id=105>
- John A. Cassara
www.JohnCassara.com

- ^{xvii} “Chinese homebuyers pump \$13.4B into California as U.S. real estate market sees resurgence of foreign investors,” Palo Alto Online, July 25, 2025; <https://www.paloaltoonline.com/real-estate/2025/07/25/chinese-homebuyers-pump-13-4b-into-california-as-u-s-real-estate-market-sees-resurgence-of-foreign-investors/>
- ^{xviii} “FinCEN Issues Advisory and Financial Trend Analysis on Chinese Money Laundering Networks,” U.S. Treasury Press Release, August 28, 2025; <https://home.treasury.gov/news/press-releases/sb0231>
- ^{xix} Sebastian Rotella and Kirsten Berg, “How a Chinese American Gangster Transformed Money Laundering for Drug Cartels,” ProPublica, October 11, 2022; <https://www.propublica.org/article/china-cartels-xizhi-li-money-laundering>
- ^{xx} Much of this section is taken from: John A. Cassara, “Flying Money May Land in the U.S.,” Banking Exchange, February 21, 2016; <https://www.bankingexchange.com/news-feed/item/6079-flying-money-may-land-in-u->
- ^{xxi} The definition of hawala was concisely expressed during the 1998 U.S. federal trial of Iranian drug trafficker and money launderer, Jafar Pour Jelil Rayhani, and his associates. The definition was coined by FinCEN analyst and expert witness Patrick Jost.
- ^{xxii} According to the World Bank, “official” global remittances totaled approximately \$625 billion in 2018. According to the IMF, “unrecorded flows through informal channels are believed to be at least 50 percent larger than recorded flows.” For a full explanation and links to original sources, see John Cassara, “Money Laundering and Illicit Financial Flows,” pages 99-103
- ^{xxiii} “Chinese Money Laundering Networks: 2020 - 2024 Threat Pattern & Trend Information,” FinCEN, August 2025; <https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf>
- ^{xxiv} “Daigou Surrogate Shopping and the Cost of Regulatory Failure,” FinCrime Central, February 16, 2026; <https://fincrimcentral.com/daigou-surrogate-shopping-money-laundering/>
- ^{xxv} Statement of Ricardo Mayoral, Assistant Director Countering Transnational Organized Crime, HSI Investigations, before the U.S. Senate Caucus on International Narcotics Control, April 30, 2024; <https://www.ice.gov/doclib/news/library/speeches/240430mayoral.pdf>
- ^{xxvi} Geeta Mohan, “How China’s Intelligence Law of 2017 authorizes global tech giants for espionage,” India Today, July 27, 2020; <https://www.indiatoday.in/news-analysis/story/china-national-intelligence-law-2017-authorise-companiesespionage-india-1705033-2020-07-27>
- ^{xxvii} John Cassara, *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails*, Amazon Kindle Direct Publishing, 2020. Each chapter covering an individual money laundering methodology or technique concludes with recommendations. In addition, see Chapter 14, “More Forward Steps,” page 315
- ^{xxviii} I go into specifics on changing the culture and incentives in my book, *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails*. See pages 316 – 318.
- ^{xxix} Carol House, “Financial Services Committee on Modernizing Illicit Finance Frameworks for the twenty-first Century,” Atlantic Council, May 21, 2026; <https://www.atlanticcouncil.org/commentary/testimony/carole-house-testifies-to-house-financial-services-committee-on-modernizing-illicit-finance-frameworks-for-the-twenty-first-century/>
- ^{xxx} Raymond Baker, *Capitalism’s Achilles Heel*, Wiley & Sons, 2005, page 173
- ^{xxxi} John Cassara, *Money Laundering*, Chapter 2 – Sobering Statistics
- ^{xxxii} John A. Cassara, *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*, Wiley, 2016
- ^{xxxiii} John A. Cassara, Written Statement for the Hearing On “Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance,” Before the Task Force to Investigate Terrorism Financing, Of the House Financial Services Committee, February 3, 2016; https://financialservices.house.gov/uploadedfiles/02.03.2016_john_a_cassara_testimony.pdf