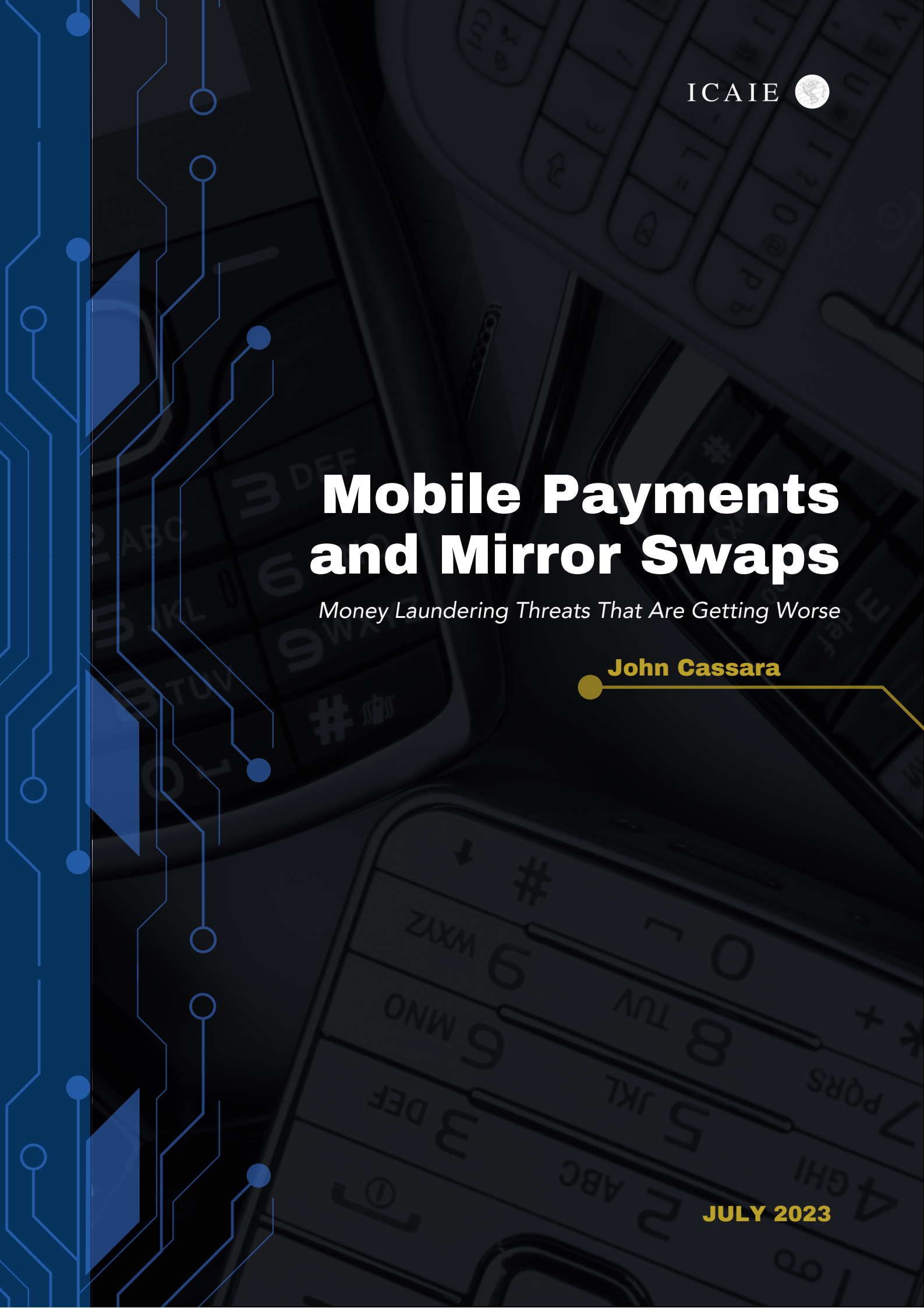


ICAIE

Mobile Payments and Mirror Swaps

Money Laundering Threats That Are Getting Worse

John Cassara

JULY 2023

CONTENTS

Introduction

In 2008, the author of this ICAIE policy brief wrote an article published by the U.S. Department of State titled "Mobile Payments —a Growing Threat."[1] In 2020, the Department of State noted that the "risk that criminal and terrorist organizations will co-opt M-payment services is real."[2] According to one U.S. criminal investigator that has first-hand experience with new forms of mobile money laundering, "it's the most sophisticated form of money laundering that's ever existed."[3]

This ICAIE policy brief will summarize mobile payments (M-payments) evolution as a money laundering methodology. The initial focus will be on the use and growth of M-payments and resultant money laundering in the developing world. The policy brief will then describe the Black Market Peso Exchange (BMPE) and the introduction of mirror swaps or the laundering of illicit proceeds via Chinese cell phone apps to facilitate money laundering worldwide. Furthermore, an assessment will be made of the current regulatory measures employed by the U.S. government to combat mobile payment laundering, along with suggestions for strengthening these countermeasures.

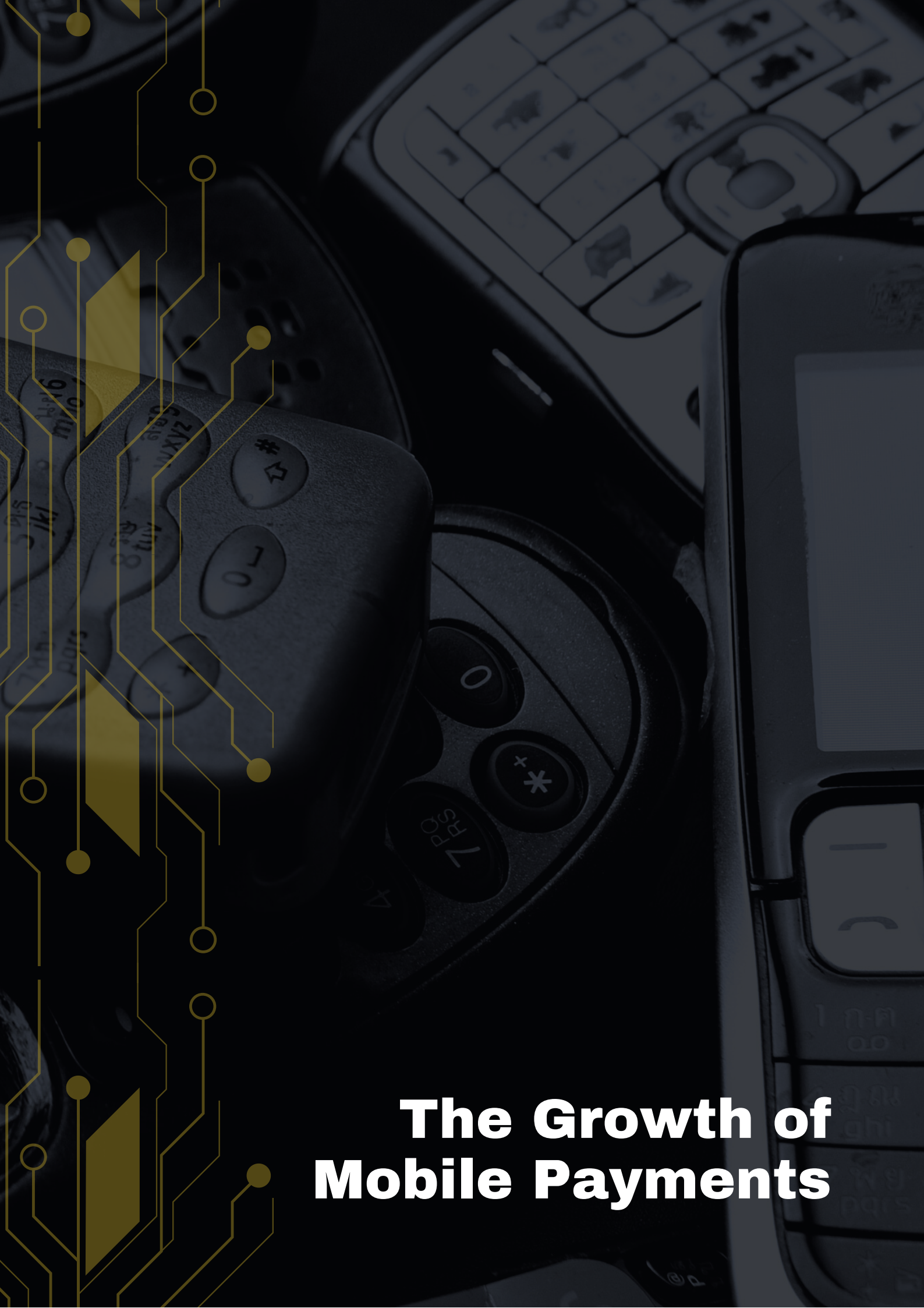
While some risks of mobile device money laundering were evident during the early stages of mobile payments, others, such as the relatively recent use of financial apps to facilitate mirror swaps, were unforeseen 15 years ago. Unfortunately, today these risks posed by various M-payment laundering techniques have been mostly ignored, allowing criminals and other malevolent actors to exploit them to move substantial amounts of illicit funds.

The stakes are enormous. The industry is growing rapidly around the world while simultaneously, M-payment laundering stymies criminal investigators. In the United States, ineffectual regulatory measures have enabled M-payment money launderers to successfully bypass financial intelligence reporting requirements—the most critical anti-money laundering (AML) countermeasure for the U.S. and the international community.

When M-payments were first introduced, the money laundering threat was mostly limited to the developing world. Over the last few years, that has changed. For example, the BMPE is one of the significant money laundering methodologies facing the United States. Clones of the BMPE have spread around the world. The BMPE is a subset of trade-based money laundering (TBML). The BMPE uses the proceeds of crime to purchase trade goods. Unfortunately, the BMPE has taken a dangerous new turn. Chinese illicit actors are increasingly working with narcotic trafficking organizations and laundering the proceeds of crime—including the sale of fentanyl—via Chinese mobile payment apps.

Note

Per a definition[4] by the Financial Action Task Force (FATF), mobile payments or M-payments is an umbrella term that covers diverse high-tech money transfer systems such as digital precious metals, internet payment services, prepaid calling cards, and payments and value transfer via the use of cell phones apps. This policy brief will specifically focus on the use of cell or smartphones (including disposable burner phones) for money laundering and value transfer, specifically within mobile network operators, where transactions such as payments, remittances, and transfers are typically processed for individuals over the operators' wireless networks. It will not address mobile payment services offered by financial institutions or the mobile payment service provider model where the provider offers mobile payment capabilities to merchants.



The Growth of Mobile Payments

The growth of access to cellular devices is breathtaking. In 1990, there were approximately 11 million mobile or cell phones worldwide.[5] In 2016, the number of mobile lines in service surpassed the global population.[6] Today more people have cell phones than electricity and running water. According to Statista, in 2023, including both smart and feature phones, the current number of mobile phone users is 7.33 billion. That means approximately 91% of people in the world cell are phone owners.[7] Similarly, the use of mobile payments via cell phones has skyrocketed.

The Groupe Speciale Mobile Association (GSMA), which includes over 1,000 mobile operators and related businesses and industries, estimates that in 2022 there were 1.6 billion registered mobile money accounts. Hundreds of millions of mobile accounts were further added during the pandemic. According to the GSMA, in 2022, approximately $3.45 billion was transacted daily via mobile money. In addition, the number of mobile money agents grew from 12 million in 2021 to roughly 17 million in 2022.

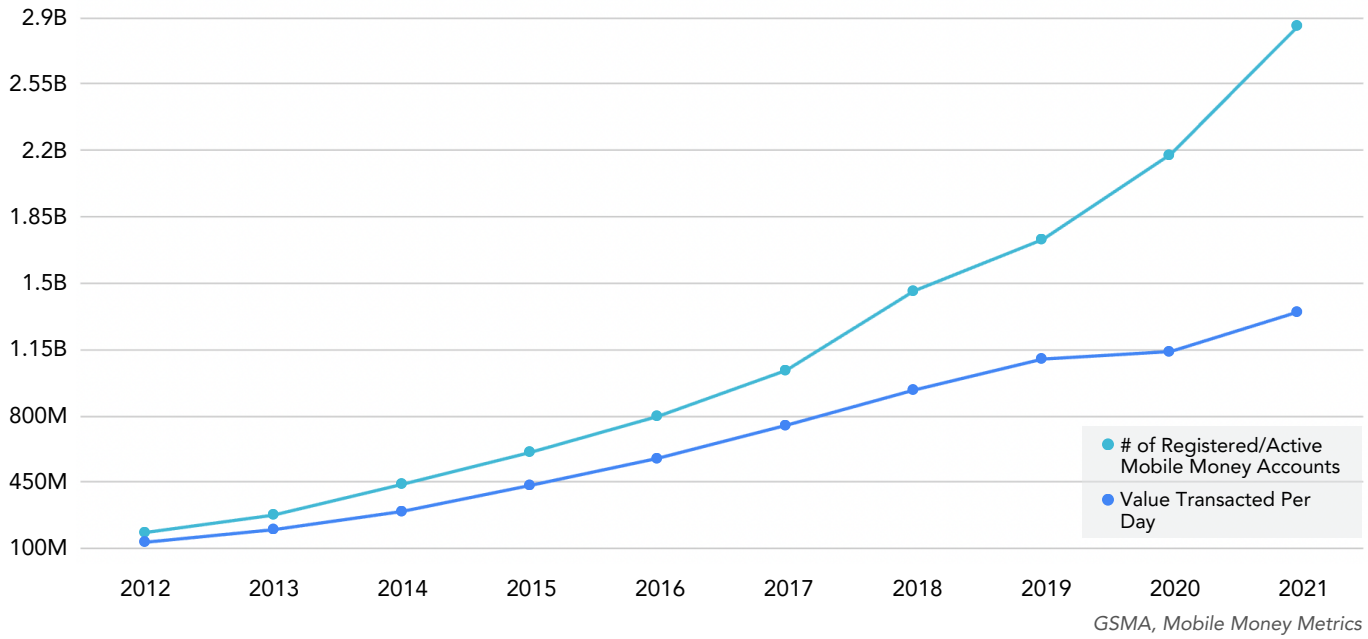
Moreover, focusing solely on remittance-related mobile transfers, the annual total value in 2022 was approximately $22 billion, exhibiting a yearly growth rate of 28%.[8]

Looking ahead, the projections for the future of the mobile payment market are equally striking. By 2030, the global mobile payment market is anticipated to reach an astounding $600 billion, indicating the ongoing upward trajectory and immense potential of mobile payments as a force in the financial landscape.

We should applaud these developments. The G-20 included "financial inclusion" in its priority agenda to help over two billion adults worldwide with limited access to financial institutions. A notable outcome of the growing use of mobile payments is the increased accessibility of mobile phones and mobile money for women in the developing world. As a result, their economic independence is bolstered, and they assume a more influential role as financial decision-makers.

M-payments' popularity stems from the wide array of secure financial services they offer, providing convenience and efficiency. For example, they allow the greater ease of purchase of products, services, the payment of bills, the transfer of money person-to-person (P2P), the facilitation of micro payments for low value repetitive goods such as mass transit, the settlement of utility bills, payment of taxes, school fees, health, and many other services. Moreover, M-payments foster transparency through their active efforts to combat fraud, extortion, and corruption while ensuring the responsible distribution of salaries and government benefits directly to cellular devices. Cell phones have also become the means for remittances from migrant workers to be sent back home. The impact of M-payments extends beyond individuals, as they generate more significant revenue for small and medium enterprises (SMEs) and empower the creation of new businesses. Mobile lending is an increasingly popular service.

Unfortunately, while cell phones are now easily available, over 1.4 billion people worldwide still do not have access to essential financial



GSMA, Mobile Money Metrics

services.[9] The disparity is evident in various regions; for example, in Africa, despite having 54 countries and 17% of the world's population, only 37% of adults across the continent have access to formal financial services, and 3% have access to the internet.[10] To illustrate even further, in Mauritania, according to the 2018 Global Findex, a little over 20 percent of the population beyond 15 years old had financial accounts. Mobile money accounts reached only 4% of adults.[11] The lack of access to financial services prevents individuals and households from escaping poverty, building wealth, and limiting overall economic growth.

Yet progress in financial inclusion has been rapid and nothing short of remarkable. Easy access to M-payments transforms lives by providing a much-needed link to contemporary financial services at a reasonable price. The beauty of these services lies in their inclusivity, as users are not required to have a bank account or credit card. Mobile banking services fill the gap and, as a result, are expanding rapidly. According to the GSMA, there are over 166 mobile service providers in Africa. As of 2022, there were 763 million registered accounts in sub-Saharan Africa, facilitating transactions valued at approximately $832 billion. On a global scale, the transaction total was approximately $1.26 trillion.[12]

Safaricom's M-Pesa, one of the world's most successful and widely adopted mobile money services, is providing innovative leadership on M-payments in Kenya and sub-Saharan Africa. In 2006, approximately when M-Pesa was initiated, Kenya had a financial inclusion rate of only 26 percent. Today the same rate is over 85%. Out of a total population of 51 million, over 23 million Kenyans use M-Pesa. There are well over 100,000 M-Pesa agents in Kenya alone. Using 2022 data, over 70 percent of Kenya's GDP flowed through M-Pesa.[13]

M-Pesa is not only Kenya's leading mobile money service provider, M-Pesa Africa has become one of the most significant companies in a vibrant African fintech ecosystem. M-Pesa Africa has expanded to seven countries and has over 50 million monthly active customers.[14]

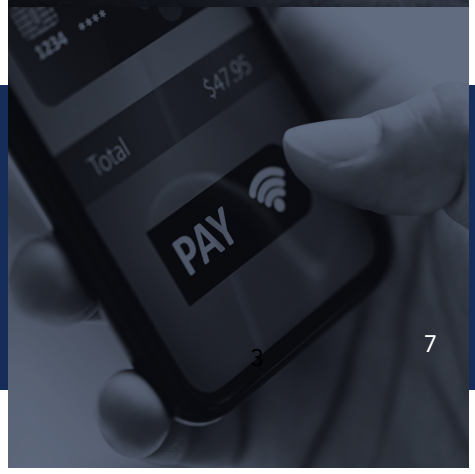
How M-Payments Work

The following is a simple summary of how money is deposited and transferred via cell phone.

1 The mobile payment user hands over cash to a designated M-payment outlet, which can be a small independent shop or convenience store found in both rural and urban areas, especially in developing countries. The user incurs a nominal fee based on the transaction amount.

2 The M-payment processing center electronically transfers the monetary credit through the mobile network operator to the recipient's mobile phone. In some cases, other forms of payments like salaries or government benefits can also be directly deposited into the recipient's mobile payment account.

3 The recipient receives a text message notification, alerting them that the transfer to their digital wallet has been successfully executed.



4 With the credited funds now available in their digital wallet, the recipient can utilize them for various purposes.

Mobile Payments and Money Laundering

Money laundering can be defined as the hiding or disguising of criminally-derived proceeds or "value" from any form of illicit activity. The keyword in the definition is *any*. Money laundering is much more than laundering the proceeds of narcotics sales. In the United States, there are hundreds of "specified unlawful activities" (SUAs) or "predicate offenses" to charge money laundering. For example, SUAs include trade fraud, weapons trafficking, human trafficking, counterfeiting, trade secret theft, medical services fraud, corruption, etc. The international standard, as championed by the Financial Action Task Force (FATF), is "all serious crimes" can be used to investigate and prosecute money laundering. There is a growing international movement to include "tax crimes" as an SUA for money laundering.

From a law enforcement perspective, examining money laundering by its three recognizable stages is helpful: placement, layering, and integration. M-payments are involved with all three stages.

The first stage of money laundering is the **"placement"** of illicit cash into a financial institution. There are many ways this occurs. One of the most prevalent methods in the United States and worldwide is "structuring," sometimes also known as "smurfing." For example, a professional money launderer divides a large amount of drug dollars into small amounts. He gives small sums of money to "runners," "mules," or "smurfs" to deposit. The transactions are done in ways that attempt to avoid government-mandated financial transparency reporting requirements.

With M-payments, criminals now have a new way to place the proceeds of crime into financial networks and the global economy. For example, a professional money launderer recruits a number of smurfs and gives them the proceeds of criminal activity. Small street sales of drugs, the proceeds of stolen property, street "taxes" (extortion or protection fees), or even suspected charitable or terror financing contributions can be laundered in this manner. The smurfs then visit M-payment establishments and utilize the illicit cash to load up their cell phones with money or "e-value" under the maximum threshold level. The runner will be directed to forward the mobile money credit to master accounts or other-directed transfers controlled by the money launderer. This particular technique has been labeled by the Asian Development Bank (ADB) as "digital smurfing." Unlike traditional money laundering methods that involve placing cash into established financial institutions or money service businesses, digital smurfing has distinct advantages in evading detection, as financial intelligence or digital footprints are rarely generated. And, practically speaking, digital smurfing's evasive nature in most countries of concern is immune to law enforcement countermeasures.

The second stage of money laundering is **"layering."** Once the illicit funds are "placed" into a financial institution, the objective is to layer the dirty money with multiple transfers and transactions, thereby confusing the paper trail. This also adds numerous levels of venue and jurisdiction for the law to deal with. Layering makes it very difficult for criminal investigators to "follow the money."

With M-payments, layering is taken to new levels. In most jurisdictions, mobile value can be transferred from one account to another and then directed to a financial institution or Money Services Business (MSB) in the host country, perhaps forwarded to another country, or potentially even an offshore secrecy haven. Mobile value can be credited to an online account or perhaps used to purchase virtual currencies or even gaming tokens in cyberspace. P2P transfers are simple, as well as overseas remittances. A myriad of formal and informal money transfer systems, such as hawala or the Chinese “flying money,” can also be added to the equation to further frustrate criminal investigators trying to follow the money trail using digital wallets and M-payments. Additionally, underground networks have embraced M-payments as a 21st century means of settling accounts between brokers. In short, layering schemes are only limited by the criminal's imagination.

The third stage of money laundering is defined as **"integration."** Once the dirty money is placed and layered, fronts for a criminal organization integrate the laundered money back into the economy. They might buy luxury vehicles, palatial homes and invest in shopping centers, the stock market, and commercial enterprises. For instance, the daughter of a notorious kleptocrat in Africa has billions of dollars in net worth. The country concerned has tremendous natural resources. The money controlled by the kleptocrat’s family could be described as the "fruits of corruption." In order to help "integrate" or legitimize the laundered ill-gotten gains, the kleptocrat’s daughter has

strategically invested in multiple countries' cell phone carriers and M-payment providers.

According to the U.S. Department of State, in the West African country of Cote d'Ivoire, funds are being laundered via these M-payment techniques. In Uganda, the State Department's report highlights that "a significant portion of financial transactions... takes place in the form of mobile money payments and transfers, which could be abused by individuals and entities engaged in money laundering, terrorist financing, or other forms of financial crime. While the Anti-Money Laundering Act of 2020 (AMLA) requires financial institutions to conduct comprehensive customer due diligence (CDD), it does not put the same requirements on mobile money transfers."[15] According to a FATF/Inter Governmental Action Group against Money Laundering in West Africa (GIABA) report on money laundering in West Africa, "authorities lack tools to monitor the movement of funds sent via mobile payment platforms. Authorities identified this as an important method of transferring funds across the region, particularly considering the large numbers of the population that do not use regular banking services. There is a lack of available data regarding the potential use of this method to transmit funds for terrorist purposes, largely due to a lack of adequate oversight of the sector."[16]

While sub-Sahara Africa is the region where mobile money has seen the most exponential growth, South Asia, the Caribbean, Latin America, and the Middle East are also rapidly expanding mobile financial services. Likewise, relevant law enforcement and financial intelligence units (FIUs) struggle to keep up with related money laundering trends. Some of the most successful introductions of M-payment systems are found in the Philippines, Bangladesh, Pakistan, and Afghanistan before the U.S. withdrawal. Some of these countries already boast millions of M-payment users.

P2P M-payments can also be used to facilitate fraud. For example, according to a FATF case study, a fraudster in the Philippines deceived a victim into believing their spouse was involved in an accident. Exploiting emotions, the victim was asked to send money using a mobile payment provider to cover the hospital bill.[17] Regrettably, scams, whereby criminals impersonate loved ones asking for emergency funds, are increasingly common. Users are mostly on their own in those situations because payment apps fall into a regulatory "gray area." The criminal in essence manipulates the victim into sending money via mobile payments

—perhaps by impersonating someone the users know. Unlike transactions conducted through credit or debit cards, these mobile payment transactions lack the protective measures and loss mitigations typically associated with traditional payment methods. This is primarily because, in a sense, the user unknowingly approves the transaction, leaving them vulnerable to financial loss.[18]

Terror financing via M-Payments is also a concern. The situation is exacerbated because, for the most part, the countries involved have extremely weak AML and Combating the Financing of Terrorism (CFT) regulatory and enforcement frameworks. For example, in 2022, the U.S. State Department noted that in Mozambique, "mobile systems are increasingly used to facilitate illicit networks, including terrorists..."[19] According to Interpol,[20] the expansion of mobile money services in Africa means that terrorists will be granted increased opportunities to use mobile money facilities to enable their activities. "As mobile money services develop in Nigeria, Ethiopia and Egypt, all of whom have faced challenges concerning terrorism, terrorist organizations will likely seek to exploit opportunities from this."[21] Interpol reports sympathetic users transferring their mobile phones to members of terrorist organizations. Terrorists exploit third-party mobile phones to transfer/receive funds to/from other co-conspirators. The terror organizations understand that third-party phones are less likely to be monitored by authorities than those belonging to designated persons. Burners or disposable phones are also used.

In addition to the above regulatory and enforcement breakdowns, due diligence practiced by mandated reporting entities such as banks, MSBs, and designated non-financial businesses and professions is generally very weak. Compounding the issue, financial intelligence units are challenged — if not ineffectual — and law enforcement and prosecutors are hampered by a lack of expertise, capacity, and resources. For example, discussing the money laundering situation in Senegal, the State Department notes that "Mobile payment systems are gaining prominence. However, resource constraints prevent effective AML/CFT supervision of these entities."[22]

Case Study

The Evolution of the Black-Market Peso Exchange

Although various schemes are used to launder illicit proceeds from the sales of narcotics in the United States, for decades, perhaps the most favored 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 gravitate to new technologies and digital innovations. For example, Chinese actors using M-payments are displacing Colombians and Mexicans as preferred money launderers.

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 Deer tractors, Bell helicopters, or 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 unlawful 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 tens of billions of dollars from their illicit operations that they annually earned 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.

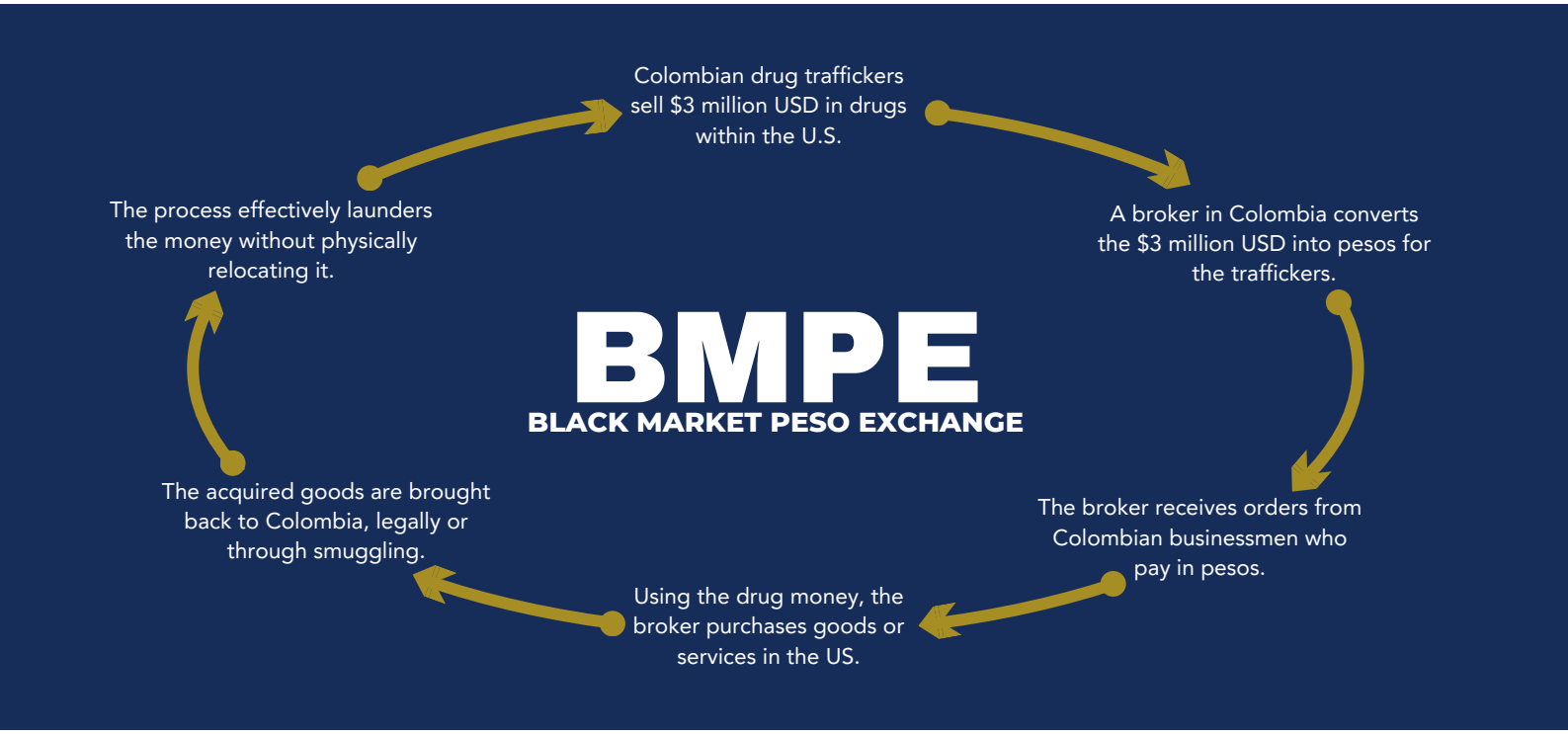
CONSIDER THIS

A Colombian drug cartel that has sold $3 million of cocaine in the United States. A cartel representative 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, obtained 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. A variety of techniques are used, including smurfing, which was described above. The money launderers design these placement techniques to avoid arousing suspicion or triggering financial intelligence reporting.

Second, the broker takes orders from Colombian businesses for U.S. trade goods. To fulfill these orders, the broker arranges for their purchase using the laundered drug money he/she owns in the United States. Some businesses should know better but are too greedy. Through "willful blindness," they don't ask the questions they should since greed is their motivation, and so they proceed with the transactions.

At the end of the day: The BMPE broker has laundered the $3 million in drug money purchased from the drug cartel.



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 money laundering investigation called Operation Fashion Police demonstrated 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 generated proceeds from narcotics trafficking remained on the U.S. side of the border. This pattern is now observed with the cartels' U.S. involvement in human trafficking, indentured servitude, kidnapping, stolen cars, organized retail theft, and other illegal activities. In return, trade goods are shipped to Mexico as part of this complex network.

About five to ten years ago, the BMPE shifted focus once again. Now, U.S. criminal investigators are finding that Chinese manufactured goods are becoming favored instruments in the BMPE. Moreover, similar BMPE financial systems with growing Chinese characteristics are found around the world to launder billions of dollars in dirty money.

In 2000, bilateral trade between China and Mexico was about 1 billion dollars. By 2021, trade between China and Mexico topped 100 billion dollars. Mexican authorities have said that the surge has allowed drug cartels and their money launderers to piggyback on this burgeoning trade relationship to expand their criminality.[23] 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, 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 is the "laundering" wash.

We see the result of this in our cities and towns, but we do not 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

licit and illicit products. A variety of goods, including electronics, garments, and small household appliances, are purchased, imported, and sold in many "China shops" and on the black market. Leveraging this form of value transfer, funds are used to buy contraband, including counterfeits, drugs, illicit cigarettes, poached ivory and other endangered and illegal wildlife and their parts, and heavily regulated flora and food items that are later shipped to China.

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. They also avail themselves of e-commerce brokers to purchase consumer products that are made in China. Chinese merchants and trading partners also practice willful blindness. They do not conduct CDD and do not care if they are being paid with illicit proceeds. Greed, again, is the driving currency for such illicit trade and money laundering.

Mobile Mirror Swaps and the BMPE

In another twist on laundering via M-payments, Chinese actors working with the Mexican cartels have pioneered the growing use of "mirror accounts" or "mirror swaps" to launder the proceeds of crime. Mirror accounts or mirror swaps are illicit methods used to launder the proceeds of crime. They involve the creation of fraudulent financial transactions that via Chinese mobile phone apps aim to obscure the true origin and ownership of illicit funds.

With "swaps," Chinese brokers often work with Chinese organized crime groups and cartels to identify Chinese/American cash-intensive businesses willing to cooperate.

How do the swaps work? The Chinese/American businessperson receives illicit proceeds from the Chinese broker working with the cartels. The broker generally has a network of businesses that cooperate, or the broker identifies customers by posting advertisements on internet bulletin boards or private WeChat forums online.[24] The Chinese-American business later "places" the proceeds of crime into its revenue flow and represents the drug cash as legitimate proceeds from the business.

In addition, the cash could be used to assist mainland Chinese citizens that want to circumvent Chinese government capital flight restrictions and, for example, purchase U.S. property, housing, or other high-ticket goods. Within China, there is growing dissatisfaction with the Chinese Communist Party (CCP) policies, such as Covid-19 lockdowns, business crackdowns, a dangerous real estate bubble, and paltry returns on savings. Many among the Chinese elites and the growing middle class are desperate to move currency out of the country. Criminal proceeds help meet the demand through these mobile mirror swaps.

The complicit businesses are asked to transfer a designated amount of money through Chinese phone apps to accounts based in China. As discussed below, this type of layering is almost impervious to U.S. law enforcement detection and countermeasures. 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 used to purchase trade goods to further the BMPE. The purchase of trade items or other tangible goods represents the final integration stage of the money laundering cycle. Or the monetary credits can be re-routed to Mexico or elsewhere per the instructions of the cartels.

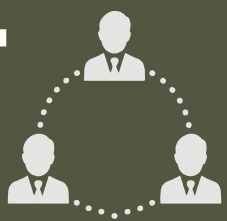
It's called a "swap" because the participating businessperson takes possession of the drug cash while simultaneously transferring the equivalent in Chinese yuan from his/her account in China to the account provided by the broker. Of course, the Chinese/American businessperson also receives a commission.

During the years of the original Colombian and Mexican BMPE, the average commission for the black-market peso broker was about 15%. The Chinese commissions average 1 to 2% on the hundreds of thousands or millions of dollars per transaction. 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.

For added security and even better tradecraft, a burner or disposable phone could be used. Mirror swaps also avoid U.S. financial intelligence reporting requirements – our primary anti-money laundering counter-measure.

How do mirror swaps work?

1



A Chinese broker collaborates with narco-traffickers and finds a willing Chinese-American businessperson.

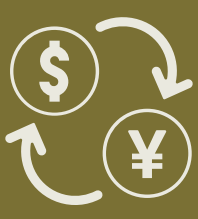
2

The businessperson receives drug cash and uses their cash-intensive business to integrate it into the financial system.

3

In exchange for a commission, the businessperson conducts transfers of equivalent amounts through Chinese phone apps.

4



Mirror swaps occur when the businessperson acquires drug cash while simultaneously transferring the equivalent in RMB from their Chinese account.

Commonly, the communications and financial transactions between the Chinese broker and the Chinese American business person occurs on WeChat, a Chinese-developed multi-purpose app by Tencent. The WeChat app contains WeChat Pay, a digital wallet similar to Zelle or Venmo that allows the user to transfer money. WeChat is very popular both in China and among overseas Chinese. WeChat is not end-to-end encrypted. Nevertheless, U.S. law enforcement is still reportedly challenged to monitor communications and monetary transactions that occur over it. WeChat's use of a form of only partial encryption still allows Tencent and the People's Republic of China's government access to content. In other words, WeChat usage is closely monitored by Chinese intelligence entities, who are at least tacitly aware of the illicit money flows. This overt use of WeChat for criminal activity like money laundering is an indicator that Beijing is aware of what is happening. The CCP's refusal to shut the networks down suggests authorities turn a blind eye to such criminality or may even profit from it. According to retired DEA Special Agent Cindric, "It is all happening on WeChat. The Chinese government is clearly aware of it. The launderers are not concealing themselves on WeChat."[25]

Case Study

Gan Xianbing and M-Payment Laundering Techniques

In 2021, a Chinese citizen, Gan Xianbing, was sentenced to 14 years in prison for his involvement in a money laundering scheme where illicit proceeds from Mexican criminal groups were picked up in Chicago, transferred to bank accounts in China, and then ultimately sent back to Mexico. The M-Payment laundering techniques used by Gan and his accomplices were nearly identical to those described above. Two other Chinese citizens, Pan Haiping and Long Huanxin, were also apprehended. They worked with Gan to launder the illicit money received in Chicago. The illicit funds were then swapped and laundered via M-payments through Chinese bank accounts. No money was ever transferred directly between the United States and China through traditional banking channels that would be subject to financial intelligence reporting.

One of Gan's associates, a Singaporean national named Seok Pheng Lim, testified she coordinated weekly pick-ups of the proceeds of crime from representatives of Mexican criminal groups. The pick-up amounts ranged between $150,000 and $1 million. The pickups were generally located in large cities, including Chicago, New York, and Atlanta. Prosecutors estimated Lim's involvement in the scheme lasted 63 weeks, during which time she and her other couriers picked up in excess of $25 million.

As described above, when Lim and others took control of the tainted cash, they worked with a network of Chinese-owned businesses in the United States and Mexico. Through M-payments, a correspondent amount of money was transferred to designated destinations through Chinese banking apps.[26]

In another case, the U.S. Department of Justice announced in July 2022 that a federal grand jury in Boston indicted eight Chinese living and working in the United States for their alleged roles in elaborate money laundering and money transmitting conspiracies, including the use of mirror swaps.[27] Tens of millions of dollars worth of drug trafficking proceeds were laundered. According to the charging documents, Qiu Mei Zeng and her former husband, Zhang, co-own China Gourmet, a restaurant in Boston's Chinatown neighborhood, were involved with the scheme. Zhang is also a registered owner of Wonderful Electronics, an electronics and restaurant supply business based in Hanover. The defendants allegedly used these businesses to run a large-scale money laundering and money-transmitting operation that involved the laundering of drug proceeds.

The defendants would accept drug proceeds in Boston and New York and, for a fee, transfer the equivalent value of Chinese RMB to drug traffickers' bank accounts and sell the drug proceeds to individuals in the United States at a discounted exchange rate. Through these off-the-books transactions, the defendants conspired to avoid United States financial intelligence reporting requirements, as well as China's capital flight limits, and to hide the nature and source of the illicit funds being transferred. In addition, according to the same DOJ press release, the conspirators used a TBML scheme that used stolen and/or fraudulent gift cards to purchase and ship thousands of Apple products, which they then shipped internationally to various locations, including Dubai, in exchange for tens of millions of dollars in wire transfers.[28]

Of course, the same type of scenario also occurs in Canada, Europe, Australia, and other parts of the world with high concentrations of Chinese nationals and businesses. Narcotics and fentanyl trafficking are often the SUA, but M-payments can be used in other predicate offenses such as human trafficking, wildlife trafficking, the sale of counterfeit goods, etc. According to the U.S. Department of Treasury's 2022 National Money Laundering Risk Assessment, M-Payments have been used to launder the proceeds of crime generated from Covid-19 fraud, economic stimulus programs, as well as unemployment/welfare fraud.[29]

ICAIE

Countermeasures and Regulatory Controls

Broadly speaking, both overseas and in the United States, there are insufficient tools to help law enforcement identify and untangle suspicious M-payments, and none are on the horizon. Mobile money transactions present many enforcement challenges because they traverse previously distinct and independent areas of regulation – particularly the telecommunications and financial banking sectors. Bureaucratically, jurisdictional issues and stove piping often involve multiple ministries and government agencies, adding much complexity to needed oversight and effective intelligence, regulatory action, and enforcement. Moreover, as noted above, there is a lack of understanding of the M-payment threat and a corresponding lack of resources and financial crime investigative capacity in most of the countries concerned.

Some skeptics might claim that there are few cases linking mobile payments with money laundering and terror finance. However, research shows that there are more and more incidents, as reported in this ICAIE policy brief as well. The frequency will assuredly increase in the coming years. Most cases are simply not recognized because the necessary technical infrastructures are not in place to trigger "red flags" or to implement meaningful AML compliance controls that may generate suspicious activity reports (SARs). There is a lack of intelligence reporting on the growing threat of M-payments as well. Over the last few years, there has been a rush by entrepreneurs and mobile payment carriers to develop the technology and deliver services while, for the most part downplaying countermeasures and procedures that could help thwart money laundering and terror financing in the first instance.

The variation in mobile money regulations between jurisdictions and the impact it has on tracking and prosecuting illegal activity that takes place across borders is a tremendous challenge. For example, if a criminal or criminal enterprise transfers money from one country to another using a mobile money service, the provider and law enforcement will only be able to track and recover funds and pursue action against the suspect/s if the criminal activities took place in countries with robust law enforcement and prosecution. Unfortunately, in most countries in the developing world where M-Payments are flourishing, the same countries are hampered by weak anti-money laundering controls, enforcement issues, lack of capacity and expertise, corruption, insufficient resources, and the absence of political will to confront money laundering seriously. Any suspicious transaction reports (STRs) filed will be routed to financial intelligence units that, for the most part, are weak and ineffectual. At the same time, the last 30 years of international AML experience consistently show that criminal networks gravitate towards the weakest link to exploit vulnerabilities.

The risks posed by M-payments can be mitigated by several countermeasures taken by service providers. Anonymity as a risk factor could be moderated by implementing robust identification and verification procedures. However, the proliferation of false identities and documentation is an increasing challenge. Imposing meaningful value limits (i.e., limits on transaction amounts or frequency) is also essential. But as noted above, criminal organizations can sometimes bypass these restrictions by structuring or "smurfing" funds.

Some service providers have implemented strict monitoring systems. For example, M-payments in the southern African country of Lesotho are flourishing. So, the Central Bank of Lesotho mandated that mobile money systems such as Ecocash and M-Pesa must adhere to the Lesotho Money Laundering and Proceeds of Crime Act. The Central Bank issued guidance that was developed to conform to "international best practices and standards." M-payment providers are mandated to follow AML/CFT compliance programs. All transactions must be local, and the amounts transferred have daily and monthly limits. In order to transfer higher amounts, know-your-customer (KYC) rules apply, and subscribers are required to present their passports and proof of their sources of income. The system also has unusual behavior triggers, which can lead to an STR being filed with the Lesotho FIU.

In October 2018, the FATF adopted changes to its recommendations to explicitly clarify that they apply to financial activities involving "virtual asset service providers" (VASPs). The amended FATF guidelines require that VASPs be regulated for AML/CTF purposes, that they are licensed or registered, and subject to effective systems for monitoring or supervision.[30] Yet years later, the updated recommendations have proven ineffectual. Across the worldwide M-payment landscape, there is no uniform standard to measure risk. AML and KYC are different in a mobile money context than they

are for traditional financial services. Many countries, jurisdictions, and providers use thresholds for transactions or caps on accounts in order to define "low-risk scenarios," but the thresholds and caps vary significantly. In addition, different views may be taken on the relevance of certain risk factors or of the effectiveness of certain risk mitigants due to respective legal and cultural differences.[31]

What is the United States government doing? The short answer is not much.

Fifteen years ago, when "the growing threat of M-payments" was first recognized, the idea of money laundering via cell phones was mostly theoretical. In the interim, Treasury's Financial Crimes Enforcement Network (FinCEN), the U.S. financial intelligence unit (FIU), was given the mandate to sort out the myriad of legal, regulatory, and enforcement issues. Little was done. U.S. regulators did make clear that existing financial services regulations apply to mobile banking and mobile payments providers. FinCEN announced "that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission" and is... "subject to relevant FinCEN regulations for AML/CFT purposes, either as part of the requirements on banks applying to all of their products and services, or as part of the requirements on money transmitters, a subset of regulated 'money services businesses."[32] As such, mobile banking and mobile payment providers are required to register with FinCEN, be licensed in most of the states where they operate, and follow traditional financial intelligence reporting norms.

Today's U.S. policies aren't working. According to the government's own data, FinCEN's MSB registration program has not been successful. "While the exact number of service providers in the United States is difficult to determine, estimates suggest that fewer than 20 percent of MSBs are registered with FinCEN. It is not known what percentage of unregistered MSBs are exempt from registration, due for example, to their low business volumes or agent status. Regardless, the result is that the vast majority of MSBs operate without direct Federal regulatory supervision."[33]

The IRS Small Business/Self-Employed (SB/SE) has been delegated by FinCEN to examine the AML program of MSBs. A total of 49 out of 50 states also have separate licensing requirements and supervision mechanisms for MSBs. Despite the above, there has been a decrease in examinations, principal exams, and FinCEN civil enforcement actions.[34]

Certainly, the diversity and accessibility of the MSB sector present challenges for regulation and oversight. Most of the businesses involved in the transfer of money through mobile devices aren't financial institutions. Some argue that companies involved in mobile payment systems that don't meet the established definition of providing banking services should not be subject to anti-money laundering enforcement scrutiny, regulation, or even consumer protection laws. Still, action needs to be taken.

For example, in the description of the BMPE and mirror accounts above, Chinese actors frequently use Chinese phone apps such as WeChat Pay and AliPay to facilitate mobile payments that represent the value of the illicit proceeds in U.S. dollars they have been given. AliPay is a registered MSB. WeChat Pay is not.[35] From a law enforcement and regulatory perspective, it would be interesting to know how many SARs have been filed—if any—by these companies and other similar M-payment service providers.

Steps Forward

The following ideas are advanced by ICAIE to encourage serious policy discussion on the development of effective countermeasures and authorities to confront the growing threat of M-Payments to U.S. national security.

Convene Panel of Experts

The issues surrounding the laundering of illicit funds via M-payments are complicated. They overlap various areas of interest and expertise. It is apparent that the U.S. government, particularly Treasury's FinCEN, is unwilling or unable to lead. The National Security Council (NSC) should convene an interagency working group to examine M-Payments, mirror swaps, TBML, and other new money laundering methodologies that are harming U.S. national security. The U.S. Congress must also have a shared responsibility in ensuring open testimony and discussions on the current law enforcement and regulatory limitations and policy shortcomings to address the threats posed by M-payments and other newer forms of money laundering in the digital world.

On a parallel track, working with other similar-minded partners, ICAIE will work with other partners to convene a group of industry and well-respected organizations and think tanks to launch an open dialogue forum where concerned law enforcement representatives, regulators, representatives from mobile carriers, and big data and analytics companies can discuss both the challenges and the opportunities of engineering AML/CFT countermeasures, policies, authorities, and procedures to address the harms associated with M-Payment systems and related criminality. Perhaps such experts could devise ways to counter the “mirror-swap” laundering method described above. Various stakeholders have roles to play and expertise to share. It’s much easier and less expensive to take proactive steps in the early stages of new financial threats rather than to wait and play "catch-up."

Mobile Payment Providers Must Become Active in AML

When it comes to AML/CFT, some mobile-payment providers are more responsible than others. But all must become active and effective. Mobile payment provider association groups should be at the forefront of an energized movement that emphasizes AML's best practices. The industry should adopt a fairly uniform and rigorous AML compliance program which includes procedures, policies, and controls that help to identify, assess, and mitigate financial crime risks, including money laundering. For those carriers that operate in multi-countries and jurisdictions, rigorous AML compliance must be standard in all locations. AML controls must involve the development of an effective CDD and KYC process, which includes the collection of customer data, risk profiling, and ongoing monitoring of transactions to detect unusual or suspicious activities. Customer identity verification is essential. In addition, AML programs should include sanctions screening, transaction monitoring, and suspicious transaction reporting mechanisms as well as robust liaison with law enforcement and/or the country’s financial intelligence unit. Mobile payment providers should also provide AML training to their employees to raise awareness about financial crime risks and the importance of AML compliance. There should be regular internal audits and assessments to make sure the ML compliance program is functioning as intended and to identify any weaknesses.

In some cases, mobile money services necessitate banking and telecom regulators to work together to allow mobile platforms to work. This type of cooperation is challenging. And while there will be some costs for the M-payment industry, M-payment providers should welcome robust anti-fraud and AML/CFT safeguards because they cannot afford to be labeled as facilitating financial crime.

Development of M-Payment AML Software

M-payments generate big data. Advanced analytics can be applied. For example, current fraud frameworks and security intelligence platforms are agile and can be adapted to various architectures and use cases. They are currently being used by both global banks and telecom companies for financial crime detection, public security, and regulatory purposes. Technology enables identity management capabilities and risk scoring using rules, predictive models, anomaly detection, as well as link and association analysis. In short, "red flags" can be engineered into M-payment systems that could automatically trigger alerts, suspend suspect transactions, and generate the filing of financial intelligence reports with the host country’s FIU. There are currently some M-Payment AML software providers. While these developments are welcome, more can be done.

Regulatory and Supervision Crackdown

M-payment providers operating within the United States are classified as MSBs. As noted, they must be registered with FinCEN, licensed in the states in which they operate, and have an AML compliance program that includes the filing of SARs.

The Director of FinCEN should convene a meeting of M-payment providers to review their AML obligations under U.S. law. Benchmarks should be announced, including the review of SAR filings. After six months, if they do not comply, their authorization to operate in the United States should be revoked.

U.S. Secret Service Should Become More Involved with M-Payment Financial Crimes

The U.S. Secret Service (USSS) has an integrated mission of protection and financial investigations. Historically part of the U.S. Treasury, the USSS protects the integrity of our currency and investigates crimes against the U.S. financial system committed by criminals around the world and in cyberspace. The USSS also has expertise in telecommunications fraud. In U.S. federal law enforcement, one entity should be given the lead for specific violations of the law. Congress should mandate the USSS expand its investigative mission to include money laundering via M-Payments. Government funding should be allocated for this purpose.

ADB	Asian Development Bank
AML	Anti-Money Laundering
BMPE	Black-Market Peso Exchange
CDD	Customer Due Diligence
CCP	Chinese Communist Party
CFT	Combating the Financing of Terrorism
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FinCEN	Treasury's Financial Crimes Enforcement Network
GSMA	Groupe Speciale Mobile Association
GIABA	Inter Governmental Action Group against Money Laundering in West Africa
KYC	Know-Your-Customer
M-Payment	Mobile Payment
MSB	Money Services Business
NAFTA	North American Free Trade Act
NSC	National Security Council
P2P	Person-to-Person
SARs	Suspicious Activity Reports
SB/SE	Small Business/Self-Employed
SMEs	Small and Medium Enterprises
STRs	Suspicious Transaction Reports
SUAs	Specified Unlawful Activities
TBML	Trade-Based Money Laundering
VASPs	Virtual Asset Service Providers

REFERENCES

1 2008 International Narcotics Control Strategy Report (INCSR) Volume II on Money Laundering, U.S. Department of State; https://2009-2017.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm

2 2019 International Narcotics Control Strategy Report (INCSR) Volume II on Money Laundering, U.S. Department of State, page 17; https://www.state.gov/wp-content/uploads/2019/03/INCSR-Vol-INCSR-Vol.-2-pdf.pdf

3 Chris Dalby, "How Chinese Criminals Secretly Move Millions for Mexico Cartels," Insight Crime, May 12, 2021; https://insightcrime.org/news/chinese-money-launderers-mexico-cartels-move-millions-secret/

4 "Money Laundering Using New Payment Methods," the Financial Action Task Force, 2010; https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingusingnewpaymentmethods.html. Note: this paper builds on an earlier 2006 FATF typologies report on mobile-payments.

5 "Electronic Finance: A New Approach to Financial Sector Development?" World Bank Discussion Paper 431

6 David Runde, "M-Pesa and the Rise of the Global Mobile Money Market," August 12, 2015, Forbes; https://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/?sh=18b7bc955aec

7 Bankmycellblog; https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

8 "The State of the Industry Report on Mobile Money, 2023," GSMA; https://www.gsma.com/sotir/#download

9 "The State of the Industry Report on Mobile Money, 2023"

10 "Pathways to expand digital financial inclusion in Africa," Bankingly, December 28, 2022; https://www.bankingly.com/news/pathways-to-expand-digital-financial-inclusion-in-africa/#:~:text=In%202022%2C%20456%20million%20adults,finance%20institutions%20or%20are%20underbanked

11 "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19," The World Bank, 2021; https://www.worldbank.org/en/publication/globalfindex

12 "The State of the Industry Report on Mobile Money"

13 "Driven by purpose: 15 years of M-Pesa's evolution," McKinsey & Company, June 29, 2022 podcast; https://www.mckinsey.com/industries/financial-services/our-insights/driven-by-purpose-15-years-of-m-pesas-evolution

14 Ibid.

15 2016 State Department International Control Strategy Report, Volume II on Money Laundering. See Cote d'Ivoire; https://2009-2017.state.gov/j/inl/rls/nrcrpt/2016/vol2/index.html

16 FATF/GIABA, "Terrorist Financing in West and Central Africa," October, 2016, page 32; http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-West-Central-Africa

17 "Money Laundering Using New Payment Methods," the Financial Action Task Force, 2010; page 40.

18 Ann Carrns, "Easy to Use, Mobile Payment Apps Are Also Easy to Misuse," New York Times, January 28, 2023; https://www.nytimes.com/2023/01/28/your-money/mobile-payment-venmo-zelle-cash-app.html

19 2022 State Department International Control Strategy Report, Volume II on Money Laundering. See Mozambique. https://www.state.gov/wp-content/uploads/2022/03/22-00768-INCSR-2022-Vol-2.pdf)

20 Mobile Money and Organized Crime in Africa, Interpol, June, 2020; https://www.interpol.int/en/News-and-Events/News/2020/Report-Criminals-infiltrating-Africa-s-booming-mobile-money-industry#:~:text=The%20'Mobile%20money%20and%20organized,illegal%20wildlife%20trade%20and%20terrorism.

21 Ibid.

22 Ibid. See Senegal section.

23 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

24 U.S. Department of Treasury National Money Laundering Risk Assessment, February 2022, page 23; https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

25 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-moneylaund

26 See Frank Main and Jon Seidel, "Chinese money-laundering rings in Chicago, New York cleaning Mexican drug cartel cash," Chicago Sun Times, April 30, 2021; https://chicago.suntimes.com/2021/4/30/22408448/chinese-money-laundering-mexican-drug-cartel-mirror-swap-trade-based-money-laundering-xianbing-gan. Also, see Chris Dalby, "How Chinese Criminals Secretly Move Millions for Mexico Cartels"

27 "Eight Indicted in Money Laundering Ring," Department of Justice, July 29, 2022; https://www.justice.gov/usao-ma/pr/eight-indicted-money-laundering-ring

28 "Eight Indicted in Money Laundering Ring," Department of Justice Press Release, July 29, 2022; https://www.justice.gov/usao-ma/pr/eight-indicted-money-laundering-ring#:~:text=BOSTON%20%E2%80%93%20Eight%20individuals%20have%20been,used%20stolen%20and%2For%20fraudulent

29 U.S. Department of Treasury National Money Laundering Risk Assessment, February 2022, pages 9 and 10

30 "Virtual Assets and Virtual Assets Service Providers," the Financial Action Task Force, October, 2021

31 "Money Laundering Using New Payment Methods," the Financial Action Task Force, 2010;

32 For more information, see "The Future of Money: Where do Mobile Payments Fit in the Current Regulatory Structure?": Hearing Before the Subcommittee on Financial Institutions and Consumer Credit, 112th Cong. (2012) (statement of James H. Freis, Jr., Director, Financial Crimes Enforcement Network, U.S. Dept. of Treasury; http://financialservices.house.gov/uploadedfiles/james_freis_testimony.pdf

33 U.S. 2007 National Money Laundering Strategy, page 3; https://home.treasury.gov/system/files/246/nmls.pdf

34 U.S. Department of Treasury National Money Laundering Risk Assessment, February 2022, page 52

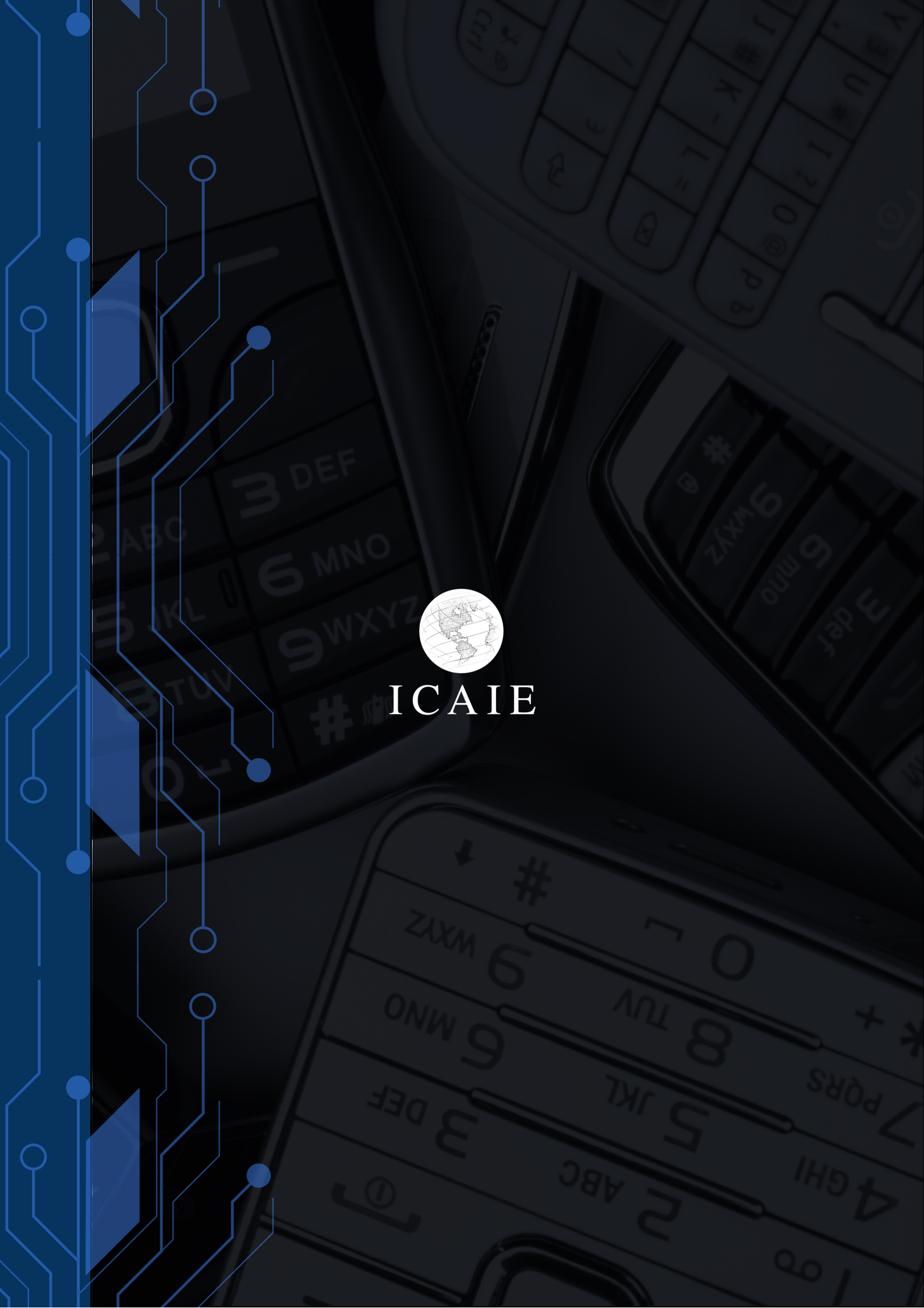
35 See FinCEN MSB search engine; https://www.fincen.gov/msb-state-selector

The **International Coalition Against Illicit Economies (ICAIE)** is a national security-centric NGO based in Washington DC that brings together committed champions across sectors and communities, including former members of the public sector, companies and prominent organizations from the private sector and civil society to mobilize collective action to combat cross-border illicit threats. ICAIE advances innovative energies through public-private partnerships, policy dialogues, and transformative threat intelligence and risk management solutions to counter illicit economies. Through ICAIE Labs, we lead a team of highly-skilled national security service providers and product vendors across the globe to examine data and open-sourced information, map illicit networks. Our multi-faceted, global investigations mine open-source data to determine identify types of illicit behavior a network may be involved in specific markets, online marketplaces, or the dark web. With an eye towards full-spectrum investigations, our ICAIE team bridges the gap between private industries and the government public sector. ICAIE Labs generate deeper investigation and supports judicial action. We leverage communications, financial, geospatial, artificial intelligence, federated learning, and other advanced analytics and technologies to investigate suspicious behavior and map networks. Ultimately, we use counter threat network operations to provide actionable intelligence, forensics, and enhanced security across the globe. Contact **David M. Luna,** Executive Director, ICAIE for additional information.

John Cassara, an ICAIE Senior Advisor, is a retired federal government intelligence and law enforcement officer with a 26-year career. He is considered an expert in anti-money laundering and terrorist financing, with particular expertise in the areas of money laundering in the Middle East and the growing threat of alternative remittance systems and forms of trade-based money laundering and value transfer. He invented the concept of international "Trade Transparency Units," an innovative countermeasure to entrenched forms of trade-based money laundering and terrorist financing. A large part of his career was spent overseas. He is one of the very few to have been both a clandestine operations officer in the U.S. intelligence community and a Special Agent for the Department of Treasury.

His last position was as a Special Agent detailee to the Department of Treasury's Office of Terrorism Finance and Financial Intelligence (TFI). His parent Treasury agency was the Financial Crimes Enforcement Network (FinCEN), the U.S. Financial Intelligence Unit (FIU). He worked at FinCEN from 1996-2002. From 2002-2004, Mr. Cassara was detailed to the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) Anti-Money Laundering Section to help coordinate U.S. interagency international anti-terrorist finance training and technical assistance efforts

Since his retirement, he has lectured in the United States and around the world on a variety transnational crime issues. He has consulted for government and industry. He has testified six times before Congressional committees on matters dealing with money laundering, threat finance, and transnational crime. Mr. Cassara is on the Board of Directors of Global Financial Integrity (GFI) and the International Coalition Against Illicit Economies (ICAIE). Mr. Cassara has authored or co-authored several articles and books.


ICAIE