BRIBERY IN INTERNATIONAL BUSINESS TRANSACTIONS
IV. CONCEALING CORRUPTION:
MONEY LAUNDERING SCHEMES

Introduction
A bribe is essentially a corrupt transaction in which some form of benefit is either paid or offered to purchase the influence of the recipient. As with other forms of corruption, bribery is generally conducted covertly to avoid detection. Thus, while any benefit may qualify as a bribe, the most common payments and offers involved in bribery schemes are those that obscure the nature of the underlying act. In addition, a system of money laundering may be employed to further conceal acts of bribery.

The international effort to combat money laundering has increased greatly in recent years due to several factors. Governments and international organizations recognize the obvious link between corruption and money laundering. The large amounts of money generated by embezzlement, extortion, bribery, and other corrupt behavior must be disguised, just as the proceeds of other forms of crime. The expanding scope of the anti-corruption movement has thus targeted money laundering as a threat to financial stability and good governance. In addition, money laundering schemes have serious implications for terrorist activities. Although terrorist groups generally do not seek financial gain from their operations, they do require funding. While some of this money comes from illegal activity, a substantial portion is contributed. The need to implement safeguards and measures to prevent misuse of financial institutions and cut off avenues for terrorist funding has significantly bolstered the campaign against money laundering. Finally, new technologies and electronic fund transfers have created new vulnerabilities. Governments have responded with stricter countermeasures that take into consideration the modern techniques used to launder money.

This chapter describes the most common forms of corrupt payments involved in bribery schemes and how the money laundering process works. An overview of the international response to money laundering follows, which focuses specifically on the work of the Financial Action Task Force. In addition, this chapter includes three case studies and a set of indicators to identify and avoid the threats posed by money laundering. It concludes with a set of review questions.

Corrupt Payment and Money Laundering Methods

Methods of Making Corrupt Payments
Certain traditional methods of making corrupt payments fall into the following hierarchical pattern:
- Gifts, travel, and entertainment
- Cash payments
- Checks and other financial instruments
Concealing Corruption

- Hidden interests
- Loans
- Payment of credit card bills
- Transfers at other than fair market value
- Promises of favorable treatment

**Gifts, Travel, and Entertainment**
Most bribery and corruption schemes begin with gifts and favors. Commonly encountered items include:

- Wine and liquor
- Clothes and jewelry for the recipient or spouse
- Sexual favors
- Lavish entertainment
- Paid vacations
- Free transportation on corporate jets
- Free use of resort facilities
- Gifts of the briber’s inventory or services, such as construction of home improvements by a contractor

**Cash Payments**
The next step usually involves cash payments. However, cash is not practical when dealing with large sums, because large amounts are difficult to generate and they draw attention when they are deposited or spent. The use of currency in major transactions might itself be incriminating.

**Checks and Other Financial Instruments**
As the scheme grows, corrupt payments are often made by normal business check, cashier’s check, or wire transfer. Payments are disguised on the payer’s books to appear as some sort of legitimate business expense, often as consulting fees. Payments can be made directly or through an intermediary.

**Hidden Interests**
In the latter stages of sophisticated schemes, the payer may give a hidden interest in a joint venture or other profit-making enterprise. The recipient’s interest might be concealed through a straw nominee, hidden in a trust or other business entity, or merely included by an undocumented, verbal agreement. Such arrangements are very difficult to detect, and even if identified, proof of corrupt intent might be difficult to demonstrate.
**Loans**

Three types of loans often turn up in fraud cases:
- A prior outright payment might be falsely described as an innocent loan
- Payments on a legitimate loan guaranteed or actually made by someone else
- An actual loan made on favorable terms, such as interest-free

**Payment of Credit Card Bills**

The recipient’s transportation, vacation, and entertainment expenses might be paid with the payer’s credit card, or the recipient might forward his own credit card bills to the payer for payment. In some instances, payers simply allow recipients to carry and use their credit cards.

**Transfers at Other Than Fair Market Value**

The corrupt payer might sell or lease property to the recipient at far less than its market value, or might agree to buy or rent property at inflated prices. The recipient also might “sell” an asset to the payer, but retain title or the use of the property.

**Promises of Favorable Treatment**

Promises of favorable treatment commonly take the following forms:
- A payer might promise a governmental official lucrative employment when the recipient leaves government service.
- An executive leaving a private company for a related government position might be given favorable or inflated retirement and separation benefits.
- The spouse or other relative of the intended recipient also might be employed by the payer company at an inflated salary or with little actual responsibility.

**Money Laundering Methods**

An inherent connection exists between money laundering and various criminal activities. Funds obtained through illegal activities must somehow be accessed without attracting unwanted attention. Money laundering is the process of disguising the origin, nature, ownership, location, or existence of illegally obtained property through a series of financial transactions. The financial transactions that comprise a money laundering scheme are common to regular business activities and, in most other contexts, are perfectly legal. However, when performed with the intent to disguise or conceal the origin of criminal proceeds, such transactions become illegitimate.

**Three Stages of Money Laundering**

Generally, money laundering is divided into three distinct stages:
Concealing Corruption

- Placement
- Layering
- Integration

**Placement**
Placement occurs when funds are first introduced into the financial system. Property obtained from illegitimate sources is most susceptible to detection and seizure during this phase. As a result, laws and regulations intended to prevent money laundering establish strict due diligence requirements and other safeguards targeting the placement of funds.

Placement can take any form. For example, a launderer can physically transport cash to a jurisdiction with relaxed financial regulations for direct deposit. Alternatively, large amounts of cash may be broken up into smaller, less conspicuous sums of money. These funds can then be deposited directly or used to purchase monetary instruments such as cashier’s checks, traveler’s checks, and money orders.

**Layering**
During layering, the launderer conducts a series of transactions to either convert the funds into another form or simply transfer them to a different location. In doing so, the launderer attempts to separate the funds from their true origin. The number of transfers involved depends on how much distance the launderer wishes to put between the cash and its source. A greater number of transfers will make tracing funds more complex, but will also increase the paper trail and the likelihood of being reported. To avoid detection during layering, money launderers rely on technological advances and banking secrecy laws.

**Integration**
Finally, integration is the phase when the assets are sufficiently removed from their criminal origin and are ready to enter the legitimate economy. Typically, the objective of a money laundering scheme is not only to disguise the source of illegal funds, but also to convert them into other assets. Seeking to a high return, a launderer may integrate funds by investing in business ventures and real estate or by purchasing luxury goods.

*Traditional Methods of Money Laundering*
There are five primary ways that money is commonly laundered. They are:
- Deposits to financial institutions
- Currency transfers
- Wire transfers
- Front businesses
- Fictitious identities
Concealing Corruption

- International transactions
- Transfers and gifts

DEPOSITS TO FINANCIAL INSTITUTIONS
The most common method of money laundering is the deposit of illegal proceeds directly into bank accounts in a financial institution. Money launderers will frequently deposit funds into business accounts without disguising the deposits as normal business receipts. This method is used primarily to transfer illegal proceeds to the business transaction system by taking advantage of the business’s bank accounts. The checks that are then written on the business account will avoid arousing the suspicion that large amounts of currency would probably generate.

By law, depository institutions are required to take measures to prevent money laundering. They must attempt to confirm the identity of customers, report suspicious activity, and meet various other requirements. However, there are many schemes by which launderers attempt to escape detection by these safeguards.

CURRENCY TRANSFERS
In attempting to identify or track down secret stores of cash, the fraud examiner is presented with a true challenge. There are several ways that currency or currency equivalents are hidden or transferred.

BULK CURRENCY TRANSFERS
The most basic method for moving cash is through bulk currency transfers, in which a person simply stores and transfers cash in hidden locations. While many launderers could use this technique, by far the largest concern is criminal organizations.

The most basic way to transport cash hordes is to smuggle them. Most countries prohibit the transfer of currency in amounts over a certain threshold (usually around $10,000) out of the country without reporting it to the government. Since launderers want to avoid these reports, they will hide the money in luggage; packages; secret compartments in cars, trucks, and freight containers; private boats and planes; and so on.

After making a series of physical transfers, criminals often enter the cash hoards into the financial institution system. This can be done anywhere, but criminals often prefer to do it in jurisdictions with less regulatory oversight. While most jurisdictions have laws to prevent criminals from successfully depositing large amounts of currency, many violations occur due to lack of enforcement or bank employees who are complicit in the laundering scheme.
For example, in 2012, an investigation into a major international bank, HSBC, revealed that criminals were using the bank to funnel large amounts of cash through its branches in Mexico. Much of this currency originated in the United States as drug proceeds. One anti-money laundering official of the bank estimated that, at one point, as much as 70 percent of the illicit currency deposited in financial institutions in Mexico was going through HSBC.

SAFE DEPOSIT BOXES
Banks and other financial institutions are frequently used by launderers as instruments for hiding or disguising assets. The methods used might be as simple as renting a safe deposit box and storing currency or valuables inside, or of a more complex nature involving transfers between banks in several countries.

Rather than conceal cash in their home, money launderers often place currency and other valuables in a bank safe deposit box. Searching the safe deposit box of a suspected money launderer for evidence requires a court order. But even if access to the box is denied, the investigator in a hidden asset case can often make educated guesses as to the contents by observing the actions of the hider. For instance, if the subject makes a visit to his safe deposit box after attending a stamp collector's exposition, the examiner could surmise he is storing a collection of investment stamps there. Trips made to a safe deposit box before foreign travel might indicate that the hider is moving money from the United States into foreign countries.

CASHIER'S CHECKS AND TRAVELER'S CHECKS
Cashier's checks are monetary instruments where the bank, as opposed to the customer, promises to pay the payee. Traveler's checks are instruments where the person signing the check can make an unconditional promise to pay the payee (unlike personal checks, which might not clear due to lack of funds). They are both often purchased for asset-hiding purposes. Because of their liquidity and near-universal acceptance, cashier's and traveler's checks are often considered currency equivalents.

Unlike personal checks that require a checking account, these monetary instruments can be purchased from some banks with cash (although many banks now require accounts, especially for cashier's checks). However, given that they may be made out in higher amounts than cash (i.e., a $10,000 cashier's check versus the $100 bill), they are more compact in transport.

These instruments are useful to money launderers for two reasons:
• They help disguise the launderer’s financial dealings and reduce the amount of currency to be carried.
• Cashier’s checks or traveler’s checks in denominations of less than $10,000 are negotiable financial instruments that can be exchanged almost any place in the world.

WIRE TRANSFERS
Several years ago, the American Bankers Association singled out unregulated wire transfers as “the primary method by which high-volume launderers ply their trade.” Suspect wire transfers are effectively hidden by the huge volume of legitimate transfers among financial institutions, which range from $1 trillion to $2 trillion daily. Electronic money laundering often requires the complicity of a foreign bank that can serve as either an intermediate or final destination of the illegal funds. Money launderers typically look for a country with a dollar economy or a place where foreign currencies are circulated freely, such as Panama, Ecuador, or Hong Kong. Especially favored are banks in the Caribbean, which are relatively or completely unregulated.

International money launderers often resort to false invoicing. Invoices for the importation of greatly overpriced goods are used as documentation to cover the electronic transfer of large sums abroad. Researchers at Florida’s International University used a computer program to detect a pattern of invoice irregularities. In one case, prices for the antibiotic Erythromycin were raised to $1,694 a gram for imports, as compared to $.08 a gram for exports.

FRONT BUSINESSES
Almost any type of business can be used for money laundering. In general terms, the businesses chosen for money laundering possess one or more of the following characteristics: revenue, expense, and history.

REVENUE
Most businesses chosen for laundering money have a revenue base that is difficult to measure because most of its revenue comes from cash transactions with a highly variable amount per customer. This allows extra money to be brought into the business and disguised as revenue.

EXPENSES
Expenses that are variable and difficult to measure can enable the launderer to extract money from the front business without giving rise to undue suspicion. The features that make such expenses good for laundering money include:
• A safe place where the movement of large numbers of people will not arouse suspicion
• Activities, such as delivery and transportation, that can be for both legitimate and illegitimate activity, but whose expenses can be entirely attributed to legitimate activity
HISTORY
Many businesses used to launder money have historical ties either with the ethnic base of a particular criminal group or with other parts of an industry—either suppliers or customers.

Businesses commonly used for money-laundering operations include:
- Bars, restaurants, and nightclubs
- Fast-food restaurants
- Vending machines and movie theaters
- Wholesale distributions
- Banks
- Money-service businesses
- Jewelry stores
- Casinos
- Mainstream businesses
- Historical businesses

FICTITIOUS IDENTITIES
An efficient way of laundering money is to establish a fictitious identity. The infant-death method is probably the most effective way to obtain a fictitious identity. In this method, the launderer acquires the identity of a same-sex person who died during childhood. The money launderer can begin the process by visiting a cemetery and finding a suitable candidate from the headstones. He then sends for a death certificate that, in many jurisdictions, is easier to get than a birth certificate. This is because less information is needed to obtain a death certificate. The death certificate shows information needed to get a birth certificate, such as the names of parents and place of birth. Armed with this information, he will then attempt to obtain a birth certificate by posing as that individual or a relative.

INTERNATIONAL TRANSACTIONS
Because some countries have relatively advantageous legal and financial climates, they are favorable to money laundering. Moreover, transferring illicit assets out of the country they were earned in is ideal for launderers to escape detection from domestic investigators. Certain European countries and the Caribbean and Far Pacific islands are well known for hidden bank accounts, fictitious corporations, secrecy, and being money laundering havens. While the United States is often viewed as the exporting side of illicit assets, as a financial center, it often serves as the receiving side of laundered assets.

Narcotics traffickers and other financial criminals who often engage in bribery use financial institutions through legitimate businesses to move the proceeds of their illegal activity out of the country. Documentation is difficult to get, and convictions are even more difficult. Once the funds leave the
mother country, it is virtually impossible to trace them. Shell companies and brass-plate banks—banks that consist merely of an office and offer no commercial banking services—abound in many countries.

Some jurisdictions allow companies to be constituted using bearer shares, a practice that can provide the owners with anonymous control of the companies. The Financial Action Task Force (FATF), an international anti-money laundering organization, asked countries to take special measures to ensure that firms with bearer shares are not used for money laundering. Several members of the FATF adopted measures to meet the FATF’s requirements. For example, the British Virgin Islands requires companies with bearer shares to have the shares deposited with an authorized or recognized custodian. Any unauthorized or unregistered bearer share will not carry any of the entitlements of a bearer share.

**TRANSFERS AND GIFTS**

Another method commonly used to dispose of bribes is to transfer assets or give them away (or at least pretend to give them away). This serves several purposes, including protecting the money from taxes, seizure, and creditors. Criminals can hide or layer assets through transfers or gifts to family members, friends, and associates. Sometimes transfers of legal title are made to stolen identities. Meanwhile, the criminal can still possess and enjoy the fruits of the illicit assets. Alternatively, the transfers could be made primarily to dissociate the assets from the launderer, in preparation for integration later on.

Charities and nonprofit organizations are also used in fraud and other financial crimes, including money laundering. These organizations rely on gifts, and therefore can be used to disguise illicit assets. Typically, the launderer or an associate controls the organization, and can direct donated funds outside of actual charitable purposes.

For example, in 2012, an Orthodox rabbi from New York was sentenced to four years in prison for his involvement in a widespread money laundering and corruption scheme. The case was part of the FBI’s “Bid Rig III” crackdown that involved the arrests of over 40 people, including politicians and other religious leaders. The rabbi ran a collection of community charities known as “gmachs.” An undercover informant approached the rabbi and sought his assistance in laundering money through the charities. The rabbi deposited check donations of almost $1 million into accounts owned by the charities. He then used an underground financial network that operated between the United States and Israel to convert the funds into cash. After taking a 10 percent commission, he physically delivered the cash to the undercover informant.

With online donations available through non-traditional transfers (such as digital currencies), it is easier than ever for launderers to make virtually anonymous payments to corrupt charities and nonprofits.
Informal or Alternative Remittance Systems

An alternative remittance system, such as the Hawala/Hundi systems and the Black Market Peso Exchange (BMPE), is a system or network of people who receive money for making it (or something of equal value) payable to a third party located in a different geographic location. Although these systems are used for legitimate reasons, they can be very appealing for misuse by money launderers.

_Hawala_, often referred to as _hundi_, is an informal remittance system primarily exploited in Asia and the Middle East. Because the system is unregulated and leaves virtually no paper trail, it is ripe for money laundering.

Hawala networks operate with the non-physical transfer of money. Typically, one who wants to send money abroad will call on a hawala dealer, known as a _hawaladar_. Hawala transactions are often disguised by legitimate businesses (e.g., travel agencies, cell phone companies, movie stores, convenience stores, and car washes). The hawaladar will contact another hawaladar in the country where the money is to be distributed, and with whom he has a familial relation or is a trustworthy connection. The hawaladars will discuss the transaction and arrange for delivery of the money to the recipient. Sometimes the hawaladar will give the giver a receipt, but with very little information. Information typically contained therein includes a code that the giver is to pass along to the recipient. Once hawaladars have exchanged the basic information of the transaction, the hawaladar for the recipient will locate and deliver the money to the recipient. The recipient will then use the code to verify his identification with the hawaladar who is distributing the money. The only records kept of the transaction are the amounts owed from one hawaladar to another. Because most hawala transactions are disguised by legitimate businesses, records of such transactions are generally disguised as well.

Typically, the network of parties in an alternative remittance system work on the basis of trust. There are often family connections between the parties. While there is little legal enforcement available to guarantee that the networked parties will live up to their agreements with the payers and payees, many people across the world rely on this system to send and receive funds. For instance, many migrant workers rely on some form of alternative remittance system to send funds to their families in their native countries. Often, hawaladars are business partners who do legitimate business with each other on a regular basis. Because it can be difficult to transfer large amounts of money between countries, a debt might be paid with merchandise or a favor (e.g., hawaladar B owes hawaladar A money from a past transaction, and pays the recipient in a new transaction, thereby relinquishing his debt to hawaladar A from the former transaction).

Compared to making and receiving transfers through normal money transfer businesses, the hawalas system has many advantages because:
• Hawalas do not require formal identification.
• The funds transferred through hawalas are available immediately, whereas banks might take up to a week to process a transfer.
• Hawala transfers are cheaper than paying bank and shipping fees because hawaladars generally take a very small commission.
• Hawalas do not require any currency conversion.
• Hawalas lack a coherent paper trail.

But because the hawala system bypasses regulation, such that money can be transferred independently of government and financial institution oversight, the system lends itself to abuse. In the case of United States v. Omian et al., the defendants pleaded guilty to owning and managing an unlicensed hawala transmittance system. In order to avoid filing Currency Transaction Reports to the federal government (mandatory for currency transactions of $10,000 or more), the defendants structured the transfers in increments under the reporting threshold. Prosecutors found that the defendants caused $9.7 million in payments to be disbursed in Yemen to unknown recipients. The original senders included individuals, businesses, and mosques.

As with the hawala systems, the Black Market Peso Exchange (BMPE), which is used by Colombian traffickers, is a Western Hemispheric variation on the informal remittance system. Very simply put, Colombian traffickers sell their U.S. dollars to black market peso exchangers, thereby effectively absenting themselves from the process and laundering their money. The BMPE exchanger has a pool of narcotics-derived dollars in the United States to “sell” to legitimate Colombian importers who are glad to get a discounted exchange rate. The Colombian merchants then use the dollars to purchase goods from the United States, which they import or smuggle into Colombia.

Technology has also come to the older alternative money movement systems. Hawala systems based in Asia and the Black Market Peso Exchange based in Colombia have migrated to the use of instant messages, chat technology, and email communications to make discovery and tracing of communications even more difficult. The absence of a traditional paper trail has always been a challenge in working with these informal money-transfer businesses, but the advent of undetectable instant global communications has made them far more difficult to monitor.

Today’s leading emerging threat is identity theft. It has all but displaced the traditional fake identity used in fraud cases, especially money laundering. It is simply far easier to assume the identity of a real person, complete with history, than it is to create a record that is as convincing. Considering that the identity is not used to gain credit or exposed to loss, there is no reason for the identified person to ever learn that the accounts were opened using his name. The risk of discovery is low, the opportunity for misdirection
Concealing Corruption

is high, and the odds of being ripped off by your victim are nil. In all, it is a near-perfect solution to the enhanced due diligence requirements being exercised by financial institutions.

Less savvy perpetrators are still using straw men, both known and random, including family members, children, in-laws, and drifters to play this role. However, the ease in gathering less traceable stand-ins makes identity theft the best bet for finding a name to use. When the scheme collapses, law enforcement will first be after the unknowing victim, who will plead amazement, allowing the actual perpetrator time to fade away. Using a drifter can be equally beneficial, but a family member will quickly bring law enforcement back to you. The unknowing victim offers the best scenario for the money launderer.

The following transactions could indicate money laundering via an alternative remittance system. The list should be used to identify those transactions that might require further investigation.

- Use of cash as payment for a transaction that is typically handled by checks or other forms of payment
- Several check deposits from various ethnic communities
- Lump-sum payments made by wire transfer or with foreign currency
- Reluctance to provide normal information when setting up a policy or account, or providing minimal information
- Purchase of investments in amounts considered beyond the customer’s apparent means
- Use of a letter of credit or other methods of trade finance to move money between countries where such trade is inconsistent with a customer’s usual pattern
- Establishment of a large investment policy and, within a short time period, customer requests cancellation of the policy and cash value paid to a third party
- Use of wire transfers to move large amounts of money to or from a financial haven country such as the Cayman Islands, Colombia, Hong Kong, Liechtenstein, Luxembourg, Panama, or Switzerland
- Services provided internationally but paid for locally

Emerging Payment Methods and Schemes

The technological landscape behind conducting transactions is constantly changing, in large part to make payments faster and more convenient. In the same way that credit and debit cards greatly changed the way people conduct common transactions, emerging payment methods are gradually gaining prominence. Also similar to the introduction of credit and debit cards, new forms of fraud and money laundering have accompanied these emerging payment methods. The same characteristics that make new payment technologies convenient for law-abiding users also draw the attention of launderers, who are always looking for new ways to conceal their criminal assets.

One of the major problems with fighting contemporary forms of money laundering is that it is often a reactionary task. Anti-fraud professionals, law enforcement, and financial regulators usually have to wait
to see what common trends and schemes develop. Unfortunately, this can mean that money launderers are often a step ahead. It is crucial for those in the financial and anti-fraud industries to keep up to date with developing methods of money laundering. Furthermore, a general knowledge of how new payment methods and technologies work is very helpful to predicting new challenges and effectively stopping them.

This section will discuss the following methods of laundering assets:

- Prepaid items
- Mobile payments
- Digital currencies

**Prepaid Items**

Many businesses offer customers the ability to prepay for products and services. This practice is beneficial to customers because it gives them the ability to give these items as gifts and also provides convenience. Moreover, prepaid items are great for businesses. They generate cash flow for items that have not been purchased yet, and some prepaid purchases are never redeemed, resulting in a windfall. Perhaps most importantly for large companies, prepaid items can open up international markets. Consumers outside the United States can use prepaid items to make online purchases with international shipping. Sometimes, the prepaid items are easier or more efficient for people outside the United States to use than dollars.

One of the biggest groups that prepaid issuers cater to is the so-called underbanked. Many people do not have or are unable to get traditional bank accounts. This is common for people with poor credit or low income, migrant workers, and others. While mainly used for legitimate business, prepaid items can also be used by money launderers to hide and transfer assets.

Broadly speaking, prepaid items are goods and services that are paid in advance of their actual purchase. Some examples of prepaid items with potential for money laundering include:

- Merchant gift cards
- Prepaid debit cards (as opposed to a standard checking/debit account)
- Payroll cards
- Prepaid mobile phones
- Mass transit cards
- Gaming and lottery cards
Prepaid items are one of the fastest growing forms of payment. According to Packaged Facts, a market research group, consumers in the United States loaded $29 billion on prepaid debit cards in 2009. In 2013, the study estimates that amount will total $202 billion. Prepaid items originally were and still are mostly issued by organizations called money services businesses—a classification that distinguishes them from traditional financial institutions because they do not engage in the same breadth of transactions. They typically provide a few types of services, such as issuing and servicing prepaid debit or gift cards. The most attractive aspect of prepaid items to bribe payers and recipients is that issuers of these items are under relatively fewer regulatory restrictions than traditional financial institutions and banking customers.

One of the most common uses of prepaid items by criminal organizations is to transfer funds out of the country. In the case of open loop items, the purchaser loads cards with illicit funds and then transports the physical card or communicates the account information offshore. The receiving party can withdraw the funds from an ATM machine or purchase items from merchants anonymously.

**Mobile Payments**

Mobile payments, also known as mobile banking, involve using a mobile phone to facilitate transactions, as opposed to cash, credit cards, and debit cards. Similar to the way in which credit and debit cards significantly cut into the use of checks and cash for consumer transactions, the successor to charge cards seems to be mobile payments.

The use of mobile phones capable of conducting transactions in the United States is the norm, and use is steadily growing in other countries, as well. Gartner, a financial research organization, estimates that mobile payment services will reach a worldwide annual value of $245 billion by 2014, up from $48.9 billion in 2010. The large-scale transition from one type of payment technology to another, unfortunately, creates opportunities for corruption. Credit card companies have had decades to modify their anti-fraud programs. Now, the less tested technology and less experienced companies involved in mobile payments will require more adjustments and solutions.

Mobile transactions are not just for purchases—they can also facilitate transfers to bank accounts or other mobile device accounts. Some carriers, including those providing prepaid phone accounts, allow users to deposit thousands of dollars into their accounts, which are then transferable. Other third parties operate digital wallets that users can transfer funds in and out of using mobile devices.

Money launderers can use mobile transfers to make anonymous, illicit bribes or to move funds offshore. Some direct billing services have a prepaid card or number associated with the account that can be used...