




BARRICK GOLD CORPORATION

**INVOICE RED FLAG
MANUAL**

	Version	Date
	2	July 15, 2014

Contributors	Name	Title	Contact
Administered by:	Kaveh Shahrooz	Corporate Counsel	kshahrooz@barrick.com
Reviewed by:	Giovanna Moscoso	Vice President & Senior Counsel	gmoscoso@barrick.com
Approved by:	Jonathan Drimmer 	Vice President & Deputy General Counsel	jdrimmer@barrick.com
Distributed to the following departments:		Legal (Corporate, Country, Sites) Finance and accounting (Corporate, Country, Sites) Authorized Approval Officers	

INVOICE RED FLAG MANUAL

The following manual is intended for use by Barrick (“Barrick” or the “Company”) employees who review, process and approve third party invoices, including Finance and Accounting. This manual is intended to provide background and guidance surrounding anti-corruption red flags, to help ensure that payments to third parties who interface with the government on Barrick’s behalf, and to the government itself, are made in a manner consistent with applicable anti-corruption laws and our policies.

Background on Anti-Corruption and Anti-Bribery

Compliance with anti-corruption and anti-bribery laws is an important element of Barrick’s strongly-held desire to operate ethically, in accordance with our values as expressed in the Code of Business Conduct and Ethics, and consistent with the law everywhere we operate. Failure to comply with the Policy and Procedure puts Barrick, its directors and officers, and individual employees at genuine risk for perceived unethical behaviour and legal liability.

Barrick operates in many environments that external observers rank as having a high risk of corruption. Of the countries in which we have operating mines, seven are ranked by Transparency International as high risk areas. Moreover, we operate in an industry that ranks high in terms of perceived likelihood of fraud and corruption and is, therefore, an area of focus for enforcement authorities.

Anti-corruption laws – the most relevant of which are the US Foreign Corrupt Practices Act (“FCPA”), Canada’s Corruption of Foreign Public Officials Act (“CFPOA”), and the UK Bribery Act – are far reaching, both in substance and geographic scope. They can be triggered when a company provides, either directly or indirectly, anything of value¹ to any government official² for any improper purpose, which essentially means getting an advantage or benefit to which that company is not entitled. The laws apply on a worldwide basis, meaning that any corruption in connection with Barrick’s operations, anywhere in the world, and committed by a parent, subsidiary, or agent, can violate anti-bribery laws.

Bribery issues can come up in a variety of contexts. These contexts include seeking licenses and permits, payment of taxes and royalties, obtaining visas, clearing customs, payments during litigation, the purchase and sale of goods, and other areas. It can also come up in the context of providing support to government officials related to the Company’s work, such as per diems, meals, entertainment, and

¹ For the purpose of the anti-corruption laws, “thing of value” includes, but is not limited to: (i) money; (ii) job opportunities; (iii) consulting agreements; (iv) contributions or donations; (v) gifts, meals, or entertainment; (vi) travel; (vii) use of cars or boats; (viii) health care or other social benefits; or (ix) scholarships. These are only examples, as many different kinds of things can be valued by someone.

² For the purpose of anti-corruption laws, “government official” is understood as any appointed, elected, or honorary official or any employee of a government, a government-owned or government-controlled enterprise, a public international organization (such as the United Nations or the World Bank), or an individual acting in an official capacity for such government, entity, or organization. The definition encompasses officials in all levels of government (local, state/province, federal) and all branches of government (executive, legislative, and judicial). The definition often also includes political parties and party officials and candidates for political office. A person does not cease to be a government official by purporting to act in a private capacity or by the fact that he or she serves without compensation. It broadly includes, without limitation: (i) politicians and their staff; (ii) judges; (iii) employees of government agencies (such as tax, immigration, mines, environment, or customs employees) and legislative bodies; (iv) employees of government-owned universities; (v) members of the police or military; (vi) public hospital or university employees; (vii) United Nations or World Bank employees; (viii) employees of private companies that are largely owned by the state, or which the state effectively controls; (ix) ambassadors and embassy personnel; or (x) private persons who may be performing a function for the government.

hospitality support. In short, any time there is an interaction between a government official and a representative of a company (direct or indirect), there is a risk that corruption issues may arise.

Third Party Invoices and Willful Blindness

Most bribery prosecutions of multi-national companies like ours do not involve direct payments by the company to a government official. Most often, something of value is provided a third party vested with authority to act on the company's behalf. For instance, it might involve a payment by a consultant to a government official in the course of seeking a license, approval, or concession. Or it may be a payment by an outside lawyer to a judge, or by an accountant to a tax authority. The costs for these illegal payments are then often passed on by the third party to the company in different ways. Sometimes, it is passed on through a success fee or commission, in which the improper payment is absorbed in the fee paid to third party. Sometimes, it is paid out of petty cash. Frequently, however, it is passed on by the third party in an invoice containing a vague description of services (or no description at all), which asks to be paid to a bank account abroad, which bypasses the third party's normal internal invoicing process, or which contains or is the product of other anomalies.

Anti-corruption laws that apply to Barrick and its employees explicitly prohibit corrupt payments made through third parties or intermediaries. Significantly, those laws do not require that an employee know the third party is making or has made a corrupt payment. Instead, individuals and companies can violate the law, and be prosecuted, where they are "willfully blind" – that is, where they are aware of facts that reveal a high probability of a corrupt payment, commonly referred to as "red flags". Where such red flags are present, individuals and companies have an obligation under the law to conduct reasonable inquiries, or they risk being prosecuted for being "willfully blind". The U.S. government has referred to this as an affirmative legal requirement to avoid the "head-in-the-sand problem". In the eyes of the Securities and Exchange Commission ("SEC"), which regulates Barrick and its employees via the company's listing on the New York Stock Exchange:

- in some circumstances a person or company can violate the law when they fail to follow up on a red flag even without a corrupt payment being made; that is, the failure to conduct reasonable inquiries is a violation of the law in its own right.
- a company can violate the law when it fails to have adequate processes in place to deter and prevent bribery, including in relation to invoices, again even without a corrupt payment being made.

Accordingly, when a red flag is present, we have an affirmative legal obligation to follow up and obtain reasonable explanations.

That does not mean, of course, that simply because a red flag appears, we cannot hire the consultant in question or make a relevant payment. But it does mean that we cannot simply ignore the red flag. We must ask questions about the facts giving rise to the red flag. As the U.S. government phrases it, the

“concerns” may not remain “unanswered,” the answers may not “raise additional concerns and red flags” that are unaddressed, and “the degree of scrutiny should increase as red flags surface.” Consistent with that approach, the stronger the red flags – and not all red flags raise equal level of concern -- the greater the degree of follow up is required before a payment can go forward.

What kinds of red flags are there?

There are many different kinds of red flags that may be present in our dealings with third parties. The U.S. Department of Justice and the SEC, in their guidance materials, offer several examples:

- excessive commissions to third-party agents or consultants;
- unreasonably large discounts to third-party distributors;
- third-party “consulting agreements” that include only vaguely described services;
- the third-party consultant is in a different line of business than that for which it has been engaged;
- the third party is related to or closely associated with the foreign official;
- the third party became part of the transaction at the express request or insistence of the foreign official;
- the third party is merely a shell company incorporated in an offshore jurisdiction; and
- the third party requests payment to offshore bank accounts.

It is for these reasons that we must monitor our payments closely, to ensure that all payments made by Barrick are to legitimate third parties and for legitimate purposes. For further guidance on red flags regarding relationships between third parties and government entities, see Barrick’s manual for Authorized Approval Officers.

What is are invoice “red flags”?

One kind of red flag, and the red flag that this manual is designed to help explain, relates to invoices or other request for payment from third parties requesting payment in cases involving the government – e.g., where (1) the government, a government official, or a relative of a government official is the payee; (2) the payee was referred to Barrick by a government official; or (3) where the payee is someone who interfaces with the government on Barrick’s behalf. Generally, an invoice red flag is an out-of-the-ordinary, or suspicious fact or detail about the size of the payment, the recipient, the service provided, or the invoice itself.

There are nine categories of red flags that you should consider when reviewing requests for a government-related payment. Any unusual element about the following can be a red flag: (1) the invoice characteristics; (2) the description of goods/services on the invoice; (3) the amount of the invoice; (4) the currency used on the invoice; (5) the payment instructions; (6) the payee; (7) the G/L account code; (8) the supporting documentation; and (9) third party relationship and activities.

A detailed (though not exhaustive) list of red flags appears in the table attached as Appendix A. Each of these listed red flags has been found in one or more cases where bribery has occurred. Each is an

indicator that some element of a payment request is unusual and requires further review and assessment. It may be a sign, for instance, that the invoice has not gone through the normal approval process, and the payee is seeking to evade detection because it reflects an improper payment. Or it may indicate that the payee is looking to hide the true nature of the services performed, or is looking to divert funds for purposes that violate anti-corruption laws or Barrick policies.

Barrick's Finance and Accounting group must review all requests for payment to High Risk Vendors,³ or which are coded to a GCOA account for Government Support Payments,⁴ for potential red flags prior to payment. Where a red flag appears in invoices that have a government connection, it is important to raise the issue to Barrick legal personnel or local compliance personnel consistent with the guidance in Appendix A. Typically it is appropriate to raise the matter with a supervisor to obtain a second opinion or verification of the red flag prior to raising the issue with legal or compliance personnel. Often, especially where the red flag by itself raises more mild questions and not significant concerns, the answer is readily apparent from the backup documentation or the vendor file. If not, legal or compliance personnel may have to obtain an explanation directly from the Barrick employee who has approved the invoice, oversaw the goods or services, or who otherwise owns the relationship with the third party, as well as legal.

Finance and Accounting should not pay any invoice coded to a high risk vendor or coded to a GCOA account for Government Support Payments unless they gain comfort that the invoice is legitimate and any identified red flags have been cleared. To be clear, because a red flag may be present does not mean that a full investigation needs to be conducted; most of the time, the backup materials, or a few specific questions to a relevant employee or the third party, can provide appropriate answers and relieve the concern that is present. Only in relatively rare situations where concerns cannot be alleviated would it be appropriate to decline payment or conduct a fuller investigation.

Where should you go with further questions?

If you have further questions about this manual or about what to do if you find a red flag in a payment request, you are encouraged to speak to your supervisor, to an Authorized Approval Officer (as defined in the Anti-Corruption Procedure), or to corporate or operating unit counsel.

³ Supply Chain, along with local compliance and ethics teams, will be identifying all high risk vendors (e.g., third parties who interact with the government on Barrick's behalf, or who are owned in whole or in part by government, government officials, or the relatives of government officials, or who are referred by a government official).

⁴ See Appendix B for a list of GCOA accounts for Government Support Payments.

APPENDIX A

Nature of Red Flag	Reason It Is A Red Flag	F&A Response
INVOICE CHARACTERISTICS		
<ul style="list-style-type: none"> ● Odd appearance (e.g., strange font/spacing, misspelling) ● Unusual notations/marks (e.g., cross-outs, white-outs, handwritten changes) ● Questionable authenticity (e.g., invoice is illegible, incomplete, cut-off, does not look genuine) ● Potential variances compared to previous invoices (e.g., different appearance, signatures) ● Potential duplicates (e.g., exact or overlapping dates between invoices, splitting of invoices) ● Unusual sequence of invoice numbers or dates (e.g., sequential numbers over a period of time) ● Potential variances in the information between the invoice and the vendor master file (e.g., differences in company name, authorized signatory, or wire information) 	<p>An invoice that seems unusual on its face is a red flag. The invoice may seem unusual in itself because of the way it looks. For instance, it may have odd misspellings, strange fonts or spacing. It may have cross-outs and white-outs, and handwritten changes. The invoice may be illegible or incomplete. Or it may simply not look real.</p> <p>The invoice also may appear odd from its context. It may look significantly different from prior invoices, the signatory may have inexplicably changed, the information may greatly differ from the vendor file, or there may be multiple invoices for the same services (eg, splitting of invoices).</p> <p>Each of these is a red flag and has been associated with cases where bribery has occurred. The red flag may indicate a payment request has not gone through, but indeed circumvented, normal internal processes for the third party. It could mean that a third party employee paid a pass through to a public official and does not want his finance and accounting personnel or supervisors to know, or otherwise does not want his company to know about the true nature of the services. Or it could mean that a Barrick employee is seeking reimbursement while claiming it is for a third party; or it could mean the third party will try to evade taxes, engage in money laundering, or some other improper conduct.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about the odd appearance of the invoice. If the supervisor agrees that the invoice appears odd, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. It may be appropriate to ask the third party to explain any odd appearances, verify that the stated services were performed, and otherwise obtain comfort that the oddities about the invoice do not indicate an improper payment.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>F&A should not pay the invoice unless they gain comfort that the invoice is legitimate, and that the oddities do not suggest the payment request relates to improper activity by the third party.</p> </div>

	<p>An odd invoice does not necessarily mean an improper payment occurred. But understanding why the invoice appears odd, and gaining assurance that it was not used to make an improper payment, would be proper steps.</p>	
DESCRIPTION OF GOODS/SERVICES ON THE INVOICE		
<ul style="list-style-type: none"> ● Characteristics of the goods/services rendered warrant extra scrutiny <ul style="list-style-type: none"> - type of goods/services themselves raise heightened risk (e.g., payments to governments, government officials or relatives, or third party intermediaries) - payment is requested to a location that does not make sense (e.g., to a country other than where the vendor is based or where the services are performed) ● Level of transparency/clarity provided by the descriptions raises questions as to the nature of the services. <ul style="list-style-type: none"> - general terms such as “miscellaneous”, “other”, “services”, “commissions”, “consulting”, and others that do not provide transparency about the goods/services rendered (i.e., the business purpose is unclear) - vague descriptions with high-risk keywords (e.g., government, gift, 	<p>Certain types of payments – including payments to governments, government officials, relatives of government officials or individuals to whom government officials request payments be made – pose elevated risks of bribery. Barrick’s anti-corruption procedures expressly cover these types of payments.</p> <p>Invoices masking improper payments often contain vague descriptions, where the actual nature of the service provided is not apparent or where a euphemism is used. Or the invoice might provide a description of services that pose clear bribery risks, or not match the supporting documentation; these also have been found in past bribery cases.</p> <p>Invoices paid to an illogical location are most often associated with tax evasion, but they also have appeared in cases where a third party seeks to avoid detection of a payment to a government official. Some locations (e.g., Switzerland, the Cayman Islands, Lichtenstein) are more illogical than others, though whenever there is a payment request to a place other than where the third party is based or where the services are performed may raise concerns.</p>	<p>For payments on their face being made to government officials, their relatives, or other high risk individuals, review Barrick’s anti-corruption procedures to ensure compliance.</p> <p>Where a red flag appears, elevate the matter to a supervisor to obtain verification/a second opinion about whether the description of goods and services raises a red flag. If the supervisor agrees that a red flag is present, information explaining the nature of the service may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the</p>

<p>clearance, facilitate/facilitation, fine, fix, payoff, inside, reward, award, benefit, special, sponsor, support, politician, kickback, incentive, premium, bonus, perk)</p> <ul style="list-style-type: none"> ● Potential variances between invoice description and the supporting documentation related to the expenses (e.g., the services on the invoice do not match the backup, or vary from the services in the contract) 		<p>invoice may be able to explain the anomalies, or it may be appropriate to ask the third party to provide an explanation that alleviates the concern and does not raise any new ones.</p> <div style="border: 1px solid red; padding: 5px;"> <p>F&A should not pay the invoice unless the invoice red flag involving the description of the goods and services is adequately explained.</p> </div>
INVOICE AMOUNT		
<ul style="list-style-type: none"> ● Unusual changes in compensation (e.g., increase despite consistent quantity/type of goods/services rendered) ● The rate(s) or value(s) for goods/services on their face do not seem reasonable (e.g., excessive rate for the type of service, round dollar values, a dollar below/above approval thresholds) ● The type of goods/services on their face do not seem reasonable in relation to the value ● Frequency and/or amount of variances between budget/estimate and actual activity 	<p>Sudden and unexplained changes to invoice amounts, or rates that seem unusual or unreasonably high, have, in past cases, included a premium reflecting a payment to a government official. Likewise, payment requests that appear unreasonably low have been associated with cases where the third party obtained a discount through government intervention.</p> <p>In addition, bribes often are paid in round dollar amounts (although the backup documentation may provide a ready explanation).</p> <p>Further, where there are significant variances from budgeted amounts, it may indicate a payment on top of the contracted services.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether a red flag is present. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the invoice may be able to explain the anomalies, or it may be appropriate to ask the third party to provide an</p>

		<p>explanation that alleviates the concern and does not raise any new ones.</p> <p>F&A should not pay the invoice unless invoice amount red flags are adequately explained.</p>
CURRENCY USED ON THE INVOICE		
<ul style="list-style-type: none"> ● Potential variances in the payment currency between the invoice and the contract (e.g. the contract stipulates that payment will be made in local African currency, but invoice requested is for payment in Swiss Francs.) ● Unusual payment currency compared to the location where goods/services were delivered (e.g., services performed in the U.S., but payment requested in Euros) ● Unusual payment requests (e.g., payment requested in multiple currencies) ● Change(s) in payment currency compared to previous transactions. 	<p>As with payments to an illogical location, payments in unusual currencies, multiple currencies, or currencies that differ from prior requests or the contract have appeared in cases involving bribery and other improprieties. They may suggest that a payment in whole or part is being routed to a government official or is related to a kickback.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether the currency request raises a red flag. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the invoice may be able to explain the currency request, or it may be appropriate to ask the third party to provide an explanation that alleviates the concern and does not</p>

		<p>raise any new ones.</p> <div style="border: 1px solid red; padding: 5px;"> <p>F&A should not pay the invoice unless currency red flags on invoices are adequately explained.</p> </div>
PAYMENT INSTRUCTIONS		
<ul style="list-style-type: none"> ● “Urgent” requests for payment ● Unusual or unexpected high-level management interest or involvement in processing payments (e.g., executive “push” or “override”) ● Unusual payment instructions (e.g., split single invoice into multiple payments, payment to a different country than the country where goods/services were delivered) ● Change in payment format (e.g., from wire to cheque payments or cash) ● Frequency and/or timing (e.g., last minute requests) of changes in payment instructions ● Questionable authenticity of changes in payment processing (e.g., wire instructions on an invoice is different from the instructions in the vendor master file) 	<p>Unusual or unexplained changes to payment instructions, and urgent requests, have in past cases been associated with payoffs. If the vendor is exerting pressure to be paid quickly, it may be a sign that the recipient is keen to avoid having his invoice closely scrutinized and subjected to internal control mechanisms, or that he has made a promise to a government official. Similarly, if management pressure (from Barrick or the third party) is being exerted to make a payment, particularly one involving the government, care must be taken that the payment is for a proper purpose. Invoices requesting cash payment likewise have resulted in improper payments, and designed to evade scrutiny.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether the payment instructions raise a red flag. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the invoice may be able to explain the anomalies, or it may be appropriate to ask the third party to provide an explanation that alleviates the concern and does not raise any new ones.</p>

		<p>F&A should not pay the invoice unless a red flag involving payment instructions is adequately explained.</p>
PAYEE		
<ul style="list-style-type: none"> ● Location of the payee bank (e.g., located in a country with a low corruption perception index score, located in a different country than the country where the goods/services were delivered) ● Use of an intermediary to process payment ● Payment to a party other than the invoicing party ● Payment to a personal account 	<p>Unusual characteristics of the payee can be a red flag.</p> <p>For example, in past cases, where a payee asks to be paid in a different jurisdiction than the one in which he is based or where the services are performed, or asks that the payment be made to a third party, it has reflected a desire to use the funds to bribe officials, or evade government regulations or detection.</p> <p>Similarly, requests that payments be made to someone’s personal account rather than a business account, particularly if that person is a government official, have been strongly connected to cases involving bribery and other improprieties.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether the payee raises a red flag. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the invoice may be able to provide appropriate answers, or it may be appropriate to ask the third party to provide an explanation that</p>

		<p>alleviates the concern and does not raise any new ones.</p> <p>F&A should not pay the invoice unless the payee red flag is adequately explained.</p>
G/L ACCOUNT CODE		
<ul style="list-style-type: none"> ● Account codes and sub-codes to classify higher risk activity (e.g., entertainment involving government employees) ● Unusual or unexpected changes to the G/L account code taking into account <ul style="list-style-type: none"> - third party involved - type of goods/services rendered - requestor/initiator or approver of the expenditure - country where goods/services were provided - frequency, regularity, volume and/or value of the transaction(s) 	<p>Anomalies involving coding are most often associated with employees involved in improper schemes. They may, based on past cases, indicate an effort to obtain personal payments.</p> <p>Unusual or unexplained changes in G/L codes can indicate an effort to evade scrutiny of the real purpose of the payment.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether the coding raises a red flag. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice or who was involved in the coding, as well as operating unit or corporate counsel.</p> <p>F&A should not pay the invoice unless coding red flags are adequately explained.</p>
SUPPORTING DOCUMENTATION (E.G., RECEIPTS, CERTIFICATIONS, TIMESHEETS, MEMORANDA)		

<ul style="list-style-type: none"> ● Incomplete supporting documentation, including in particular no contract for higher risk vendor (e.g., connected to government) ● Consistency of supporting documents with type of documentation previously provided ● Consistency between the supporting documentation and the invoice in key areas (e.g., date, type of goods/services delivered, amounts charged, location, etc) ● Format of the supporting documentation (e.g., photocopy if an original is expected) ● Questionable authenticity of supporting documents (e.g., illegible, incomplete, cut-off, altered) ● Unusual notation/marks (e.g., cross-outs, white-outs, handwritten changes) on the supporting documents ● Pattern of missing documentation for same vendor ● Same supporting documentation provided across different third parties or transactions ● Resubmitting previously flagged documents 	<p>Barrick’s anti-corruption procedure requires that certain types of high-risk payment requests be accompanied by supporting documentation. Perhaps the most important category of backup documents is a contract for a high risk third party. Other types of backup documents include receipts, support agreements, rosters, AFEs, POs, and other materials that may be required for any given transaction.</p> <p>The supporting documentation is required to ensure that the payments are consistent with what has been agreed with the third party, the law and Company policies. Often bribes and other improper payments lack adequate, consistent, or any backup documentation. Sometimes, backup documents for a different service are substituted to try to hide the true nature of a payment, or the same backup materials are submitted for different transactions for reasons that are not clear. Sometimes, backup documents are forged to hide their absence, and thus raise red flags for the same reasons that odd appearances on invoices (as above) raise red flags. Any effort to obtain payment without adequate documentation, or with documentation that is questionable in its authenticity, should be viewed as a red flag.</p> <p>Questionable or unusual supporting documentation for a payment can indicate that the vendor is looking to avoid scrutiny or to purposely hide the true purpose of the payment. They are a hallmark of bribery cases.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether the discrepancies or absences in the backup documents raise a red flag. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the invoice may be able to explain the anomalies, or it may be appropriate to ask the third party to provide an explanation that alleviates the concern and does not raise any new ones.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>F&A should not pay the invoice unless there is adequate supporting documentation, and any red flag identified is adequately explained.</p> </div>
---	--	--

THIRD PARTY RELATIONSHIPS AND ACTIVITIES

<ul style="list-style-type: none"> ● Frequency, regularity, and/or volume of activity with the third-party, taking into account <ul style="list-style-type: none"> - relationship with the third party (e.g., new vs. established vendor, active vs. dormant vendor) - location of the third party (e.g., in a country with a low corruption perception index score) - goods/services provided by the third party (e.g., office supply provider vs. lobbyist) - value of the transaction(s) - contract amounts - budgets ● Incomplete or unusual third party information (e.g., no physical address, no phone number, third party information coincides with employee information) 	<p>Certain third parties, particularly those with whom Barrick has not done much business in the past, and who are related to higher risk payments, generally will not have much track record, or have not built up a relationship of trust. Invoices from new vendors, particularly those with large contracts to provide services which could lend themselves to corrupt practices, should be scrutinized more closely than established vendors operating in lower risk industries and jurisdictions.</p> <p>If any critical information about the payee is missing, it may indicate that the third party is not a genuine entity, a shell company, or otherwise not a legitimate operating entity. Such non-legitimate entities are a common feature of bribery prosecutions.</p>	<p>Elevate to a supervisor to obtain verification/a second opinion about whether the third party raises a red flag. If the supervisor agrees that a red flag is present, information explaining the red flag may appear in the backup documentation or the vendor file. If not, the matter should be raised to legal or compliance personnel. Legal or compliance should contact the employee who approved the invoice and/or the employee who owns the relationship with the third party, as well as operating unit or corporate counsel. The employee who owns the relationship or approved the invoice may be able to explain the anomalies, or it may be appropriate to ask the third party to provide an explanation that alleviates the concern and does not raise any new ones.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>F&A should not pay the invoice unless the third party red flag is adequately explained.</p> </div>
---	--	--