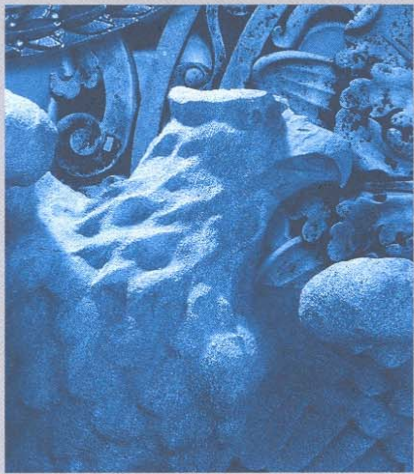


HERRICK

New York Office
2 Park Avenue
New York, New York 10016
Phone: (212) 592-1400
Fax: (212) 592-1500

Princeton Office
210 Carnegie Center
Princeton, New Jersey 08540
Phone: (609) 452-3800
Fax: (609) 520-9095

Newark Office
One Gateway Center
Newark, New Jersey 07102
Phone: (973) 274-2000
Fax: (973) 274-2500

www.herrick.com

FINANCIAL INSTITUTIONS ALERT APRIL 2008

Two Key Current Money Laundering Issues for Banks

In this Alert, we will review two key current money laundering issues, trade-based money laundering and the use of third-party checks to launder money, with some suggested procedures to assist in preventing and detecting these illicit activities.

Trade-Based Money Laundering

Trade-based money laundering is the process of disguising the proceeds of crime through the use of what appear to be legitimate trade transactions, often by misrepresenting the price, quantity or quality of imported or exported goods. Examples of trade-based money laundering include:

- <u>Over- or under-invoicing of goods and services</u>: The key element of this technique is misrepresentation of the price of goods or services in order to transfer additional value between an importer and exporter.

- <u>Multiple invoicing of goods and services</u>: This technique involves issuing more than one invoice for the same transaction, thereby justifying multiple payments. Employing several different financial institutions to make these additional payments makes these transactions even harder to detect.

- <u>Over- or under-shipments of goods and services</u>: The key element of this technique is misrepresentation of the quantity of goods being shipped.

- <u>Falsely described goods and services</u>: This involves misrepresentation of the quality or type of goods or services.

Financial institutions participate in trade financing by providing pre-export financing, issuing or confirming letters of credit, discounting drafts and acceptances, or offering fee-based services such as providing credit information on buyers. Because trade-finance is more document intensive than many other banking activities, it is more susceptible to documentary fraud, which can be linked to money laundering and terrorist financing.

There are a number of red flags that may help reveal trade-based money laundering activities, including:

- Significant discrepancies between (a) the description of the goods on the bill of lading and the invoice; (b) the description of the goods on the bill of lading or invoice and the actual goods shipped; and/or (c) the value of the goods reported on the invoice and their fair market value.

- The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities.

HERRICK

- The type of commodity being shipped appears inconsistent with the exporter's or importer's regular business activities.

- The type of commodity being shipped is at high risk for money laundering (e.g., high-value, low-volume goods which present valuation difficulties).

- The shipment does not make economic sense (e.g., the use of a 40-foot shipping container to transport a small amount of low value goods).

- The commodity is transshipped through one or more jurisdictions for no apparent economic reason.

- The method of payment appears inconsistent with the risk characteristics of the transaction (e.g., the use of an advance payment to a new supplier for a shipment from a high risk country).

- The customer directs payment of proceeds to an unrelated third party.

- The transaction involves the receipt of a payment from a third party entity that has no apparent connection with the transaction.

- The transaction involves the use of repeatedly amended or frequently extended letters of credit done for no apparently legitimate reason.

You will need sound customer due diligence procedures to gain a thorough understanding of a trade-based customer's underlying business activities, and your role in a trade-based transaction will dictate the appropriate degree of due diligence. For example, issuing banks should conduct sufficient due diligence on prospective import or export customers before providing a letter of credit. The due diligence should include gathering sufficient information on both the applicant and beneficiary, including their identities, nature of business and, if possible, sources of funding.

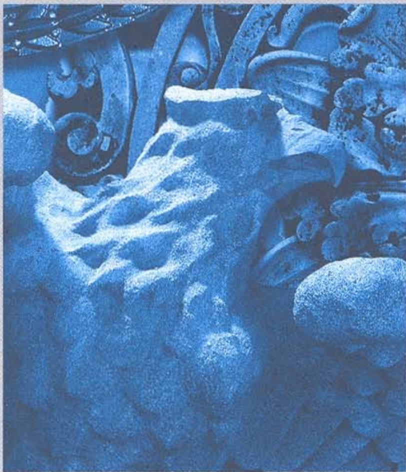
Trade finance transactions frequently involve the use of Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages. Banks need to monitor the names of the parties contained in these messages and compare those names against OFAC lists, government lists of known or suspected terrorists or terror organizations, and any internal bank lists of known or suspected money launderers.

Bank procedures should also require a thorough review of all applicable trade documentation to check for discrepancies and irregularities. The sophistication of the documentation review process should be commensurate with the size and complexity of the bank's trade finance portfolio.

Third-Party Checks

Banks always need to be aware of the potential for money laundering through the use of third-party checks. A third-party check is a check made payable to a payee who then transfers the rights to the check to a third-party by endorsing the check over to that third-party. Many individuals and businesses have legitimate reasons for using third-party checks for their transactions, but such checks are also often used to launder illicit funds. For example, bank regulators have reported that

www.herrick.com



HERRICK

significant numbers of U.S. dollar third-party checks have been presented to banks located overseas, even though both the payee and payor appeared unconnected to the country where these checks were presented for payment. When negotiated, the checks became part of international letter packages sent to correspondent banks in the U.S.

Keep an eye out for the following possible indicators of third-party check abuse:

- Checks payable to payees with no connection to the city, area or country where the checks are cashed or deposited.
- Checks for unusually large amounts.
- Checks from a bank based in a jurisdiction different from the residence of the payor, particularly where there is no apparent connection between the issuer (payor) and beneficiary (payee) of the check.
- Checks written for amounts just below currency reporting requirements, which are then cashed out.
- Checks that appear to have no legitimate commercial purpose.
- Multiple endorsed third-party checks used for the settlement of a single purchase or transaction.
- Multiple checks from the same payor to the same payee, but with different payor signatures on each check.
- Multiple checks from the same payor to the same payee, often consecutively numbered, but with different signatures and handwriting on the payee endorsements.
- Checks made out to different payees, often from the same payor, but bearing the same handwriting on the payee endorsements.
- Checks dated several weeks or months before the deposit date.

A careful consideration of these "red flags" will help banks to identify and minimize third-party check abuse.

For more information on these issues or other compliance or regulatory matters, please contact:
David Rosenfield at 212.592.1513 or drosenfield@herrick.com

Copyright © 2008 Herrick, Feinstein LLP. Financial Institutions Alert is published by Herrick, Feinstein LLP for information purposes only. Nothing contained herein is intended to serve as legal advice or counsel or as an opinion of the firm. Prior results do not guarantee a similar outcome.