FINANCIAL INTEGRITY NETWORK

Financial Integrity Network Policy Alert
DFS Rebuke of Pakistani Bank's New York Branch Implicates Head Office

Summary:

The New York Department of Financial Services (DFS) and the New York branch of Pakistan's Habib Bank Limited (HBL) last week entered into consent order after DFS found that the bank's compliance function is "dangerously weak" and identified strategic deficiencies in the bank's enterprise-wide risk management, including at the head office in Karachi. As a part of the consent order, HBL agreed to pay a $225 million fine, illustrating both the regulatory risks associated with foreign banks' U.S. branches and the reputational risks that arise when a U.S. regulator issues an enforcement action against a U.S. branch that implicates the internal controls at the head office. HBL also agreed to close its New York branch, but DFS will continue its probe.

Banks – especially U.S. branches of foreign banks – should draw three key lessons from the enforcement action against HBL:

- They should implement anti-money laundering/countering the financing of terrorism (AML/CFT) and sanctions compliance programs consistent with global standards across their enterprises, even if the global standards exceed what the home regulator requires;
- As legally permissible, they should make sure they are sharing information across their enterprises, especially lists of clients blacklisted for financial crimes concerns; and
- They should continuously monitor correspondent relationships for indications that a correspondent's business or risk profile has changed or is inconsistent with information obtained during onboarding.

Foreign banks – even those that do not have U.S. branches – should also take notice of the enforcement action. DFS criticized HBL's New York branch for being unaware that a correspondent was nesting relationships and for not having enough substantive discussions about the relationship with the correspondent. In a correspondent relationship, both banks are responsible for clearly understanding the obligations of each bank. Managing the risks arising from the relationship is a shared obligation. Foreign banks that fail to discuss ahead of time changes in the nature of their business or changes in how they plan to use the correspondent account expose their U.S. correspondents to real and regulatory risk and may have difficulty maintaining correspondent relationships.

Enforcement Action:

The DFS consent order is a result of intense scrutiny of HBL that began more than a decade ago. In 2006, HBL entered into an agreement with the Federal Reserve Board (FRB) after the FRB found "significant deficiencies" in HBL's sanctions and Bank Secrecy Act (BSA) compliance programs. DFS said that HBL has struggled to comply with the agreement. A 2016 joint examination with the FRB concluded that "Habib Bank and the branch's management failed to establish an appropriate [Bank Secrecy Act/anti-money laundering] control environment to manage its high-risk client base, and that the branch's management's risk appetite substantially exceeds the control measures in place at the branch," according to the DFS consent order.

In the hearing notice that DFS issued to HBL in August, DFS concluded that "the evidence … demonstrates that compliance failures found at the New York Branch are serious, persistent and apparently affect the entire Habib banking enterprise. They indicate a fundamental lack of understanding of the need for a vigorous compliance infrastructure, and the dangerous absence of attention by Habib Bank's senior management for the state of compliance at the New York branch." DFS found deficiencies across the compliance function at the New York branch. The consent order focuses on (1) insufficient risk-based foreign correspondent due diligence, (2) inadequate sanctions screening, (3) books and records violations arising from wire stripping, and (4) a failure to manage risk across the enterprise.

First, the 2016 examination revealed a variety of control deficiencies in the branch's customer due diligence program for existing correspondent customers, DFS said. The correspondent file for at least one foreign bank did not include detailed information about the correspondent's customers or a thorough review of the correspondent's actual activity against its expected activity. This could signal an evolution in regulatory expectations for the industry. In the case of HBL, the New York branch failed to detect that one of its correspondents was nesting activity for its own foreign branches in third countries, DFS said. Bi-weekly calls with the same correspondent were primarily administrative rather than focusing on jointly managing the risk posed by the relationship, according DFS's review of the minutes of the calls.

Second, DFS found serious deficiencies in HBL's sanctions compliance program:

- At least $250 million worth of transactions were excluded from sanctions screening because the parties were included on HBL's "good-guy" list. Terms on the "good guy" list included terms on the SDN list that corresponded to an Iranian oil tanker, an international arms dealer, and a designated terrorist, according to DFS.
- More than 10,000 wire transfers omitted information essential to screening, such as the names of the beneficiary or recipient.
- DFS also determined that the screening system itself was insufficient because it did not capture enough name variations. DFS cited to its longstanding compliance requirement in the hearing notice rather than the newer, more detailed requirements that came into effect this year, though screening programs capable of identifying name variants are a component of the new requirements.

Third, DFS's investigation uncovered instances of wire stripping, which resulted in at least one payment involving a Chinese weapons manufacturer subject to U.S. nonproliferation sanctions, DFS said. In that case, trade finance documents were altered to conceal that the goods being shipped were explosives. DFS also found a separate instance in which a payment was canceled and then resent to omit a prohibited party's name.

Finally, HBL failed to manage risk across its enterprise, according to DFS. Notably, the New York branch was not using the AML blacklist that its head office in Karachi was using. As a result, a transaction involving a cybercriminal on the FBI's most wanted list alerted in Karachi specifically because the customer was on the bank's AML blacklist, but the New York branch improperly cleared an alert that was generated in New York. The New York branch cleared $27,000 worth of payments for the cybercriminal, according to DFS. DFS concluded that the head office failed to provide proper guidance and oversight for the New York branch and that "the Branch management's risk appetite substantially exceeds the control measures in place at the Branch." DFS also criticized the head office's screening program: "Head office screening, which the branch has repeatedly relied on as an excuse for its own lax attitude regarding BSA/AML safeguards, appears to be as weak as that of the branch itself – if not even more inadequate."

HBL said in a statement that it "remains committed to strengthening its compliance process, operations, and controls."

Recommendations:

Correspondent banking has been an area of intense examination focus for some time. The findings against HBL illustrate the regulatory risk associated with correspondent banking and show that U.S. regulators' reach can extend to the home office of foreign banks with U.S. branches, demonstrating the reputational risks that could arise from any mismanagement of a U.S. branch. At U.S. branches of foreign banks and for U.S. headquartered banks with foreign branches or subsidiaries, risk management must be an extension of – and tightly integrated with – risk management across the enterprise. For all correspondent relationships, managing risk is a shared responsibility between the correspondent and respondent. Failures to manage risks arising from correspondent relationships jeopardize banks' connectivity to the international financial system.

Global standards cover enterprise-wide risk management extensively, because identifying illicit financial activity depends on information sharing and group-wide implementation of sound AML/CFT and sanctions compliance programs. Policies, procedures, systems, and controls must work together to deliver a full picture of a financial institution's risk. FATF Recommendation 18 provides a framework for enterprise-wide risk management that is a sound basis for developing enterprise-wide risk management policies and procedure. Recommendation 18 calls for:

- Policies and procedures for sharing, safeguarding, and using information across the group, including for group level compliance, audit, and AML/CFT functions;
- Development of internal policies, procedures, and controls, including compliance management arrangements and screening policies to ensure high standards when hiring employees;
- Ongoing employee training;
- An independent audit function to test the system in each affiliate within the group; and

- A compliance officer at a management level for each affiliate within the group.

Information sharing is a key FATF requirement because it cuts across so many of the recommendations. FATF is currently developing guidance on groupwide information sharing within financial institutions and information sharing between financial institutions.

When domestic laws covering the home office inhibit group-wide information sharing or prevent the effective implementation of group-wide risk management policies, the U.S. branch must be made aware of these problems and implement policies and procedures to address the illicit finance risks. Banks, meanwhile, should work with their home jurisdictions to change laws that are obstacles to information sharing and effective group-wide risk management. The Financial Integrity Network (FIN) has extensive experience working with banks and regulators to identify and address obstacles to information sharing.

For all correspondent accounts, whether held at a bank's foreign branch or at a foreign bank, risk management is a shared responsibility. U.S. branches of foreign banks should treat the home office as it would any other correspondent for financial crimes compliance (FCC) purposes. From the outset of a correspondent banking relationship, the parties involved must clearly understand the FCC responsibilities of each institution. Correspondents must also understand respondents' illicit finance risks and assess the efficacy of respondents' AML/CFT programs. FIN has developed a correspondent banking questionnaire for its clients to help them gather, assess, and document respondents' illicit finance risks and FCC efforts according to global standards.

Banks should also recognize that risk management is an ongoing process, and correspondents and respondents should have frequent discussions about the illicit finance risks their institutions face and the steps that they are taking to mitigate those risks. Respondents should use these discussions to inform correspondents about anticipated changes to their business, especially changes that will have a direct impact on the nature of transactions moving through the correspondent account. A bank that fails to recognize, document, and mitigate changes in the nature of transactions in a correspondent relationship incurs a higher degree of real risk and of regulatory risk. Banks are particularly cautious about correspondent banking in the current regulatory environment – especially in the United States – and respondents that fail to disclose material changes in their business are at a higher risk of losing their correspondent accounts than respondents that have an open dialogue with their correspondent banks.