

## Federal Agency Settlements with Wells Fargo Illustrate Sanctions Risks Involving IT Systems

April 14, 2023

### Key Points

- On March 30, 2023, OFAC announced a settlement agreement with Wells Fargo for 124 apparent violations of three different sanctions programs (Iran, Syria and Sudan), all related to a legacy Wachovia Bank software platform, Eximbills. OFAC deemed these apparent violations “egregious,” and Wells Fargo agreed to remit \$30 million to settle its potential liability.
- On the same day, the Fed announced a settlement agreement involving a separate penalty against WFC, Wells Fargo’s parent company, of \$67.8 million, for inadequate oversight of sanctions compliance risks at its subsidiary bank, related to the same software program. The total penalty announced by both agencies is approximately \$97.8 million.
- According to OFAC and the Fed, between 2010 and 2015, an unidentified European bank processed 124 non-U.S. dollar transactions involving sanctioned parties connected to Iran, Sudan and Syria using a Wells Fargo software platform (inherited from Wachovia), for a total of approximately \$532 million. U.S. law prohibits such transactions if performed by Wells Fargo or other U.S. persons.
- Both OFAC and the Fed determined that Wells Fargo’s risk-management and oversight functions should have identified and addressed the legal and compliance risks associated with providing Eximbills to the European bank.
- These enforcement actions demonstrate federal regulators’ focus on prosecuting the “facilitation” of sanctions-violating transactions involving IT systems.
- Compliance personnel should review their sanctions policies, training and auditing procedures, being mindful that violations might arise from legacy IT systems.

### The Settlements with Wells Fargo

The settlement agreements with Wells Fargo Bank, N.A. (Wells Fargo) and Wells Fargo & Company (WFC) involve apparent violations of three sanctions programs (Iran, Sudan and Syria), which occurred between 2010 and 2015. These violations stemmed from Wells Fargo’s 2008 acquisition of Wachovia, a U.S. bank that had an existing relationship with a European bank identified in the notice only as Bank A.

### Authors

**Jonathan C. Poling**  
Partner  
jpoling@akingump.com  
Washington, D.C.  
+1 202.887.4029

**Charles F. Connolly**  
Partner  
cconnolly@akingump.com  
Washington, D.C.  
+1 202.887.4070

**George E. Pence**  
Senior Counsel  
gpence@akingump.com  
Los Angeles  
+1 310.552.6475

**Jennifer S. Garrett**  
Counsel  
jgarrett@akingump.com  
New York  
+1 212.872.1065

**Blair Austin Campion**  
Associate  
bcampion@akingump.com  
New York  
+1 212.872.7428

**Thomas J. McCarthy**  
Partner  
tmccarthy@akingump.com  
Washington, D.C.  
+1 202.887.4047

**Peter I. Altman**  
Partner  
paltman@akingump.com  
Los Angeles  
+1 310.728.3085

---

According to the settlement agreements, Wachovia, and then Wells Fargo, used a specific trade insourcing platform called Eximills, which Wachovia tailored specifically for Bank A to “host” on Bank A’s own systems, in part so that Bank A could process international trade finance instruments involving jurisdictions sanctioned by U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC). Wachovia had actual knowledge of Bank A’s use of Eximills to evade U.S. sanctions, even creating a mechanism through which transactions involving U.S.-sanctioned persons or jurisdictions would be routed directly to Bank A, and away from Wachovia. Although Wachovia had intended to separate itself from Bank A’s transactions that would run afoul of U.S. sanctions, Bank A continued to rely upon Wachovia’s, and later Wells Fargo’s, information technology (IT) infrastructure in connection with these transactions.

Following Wells Fargo’s acquisition of Wachovia, Wells Fargo personnel raised concerns about these activities on multiple occasions, starting in or around 2012, including to senior management, about potential sanctions-related risks associated with Eximills, recognizing parallels between the scheme and recent landmark OFAC enforcement actions against ING Bank and HSBC.

Wells Fargo conducted numerous, years-long internal reviews and audits regarding the platform. Finally, in 2015, Wells Fargo identified during a business review that Bank A may have been processing transactions involving sanctioned jurisdictions and persons through Eximills. In December 2015, Wells Fargo suspended Bank A’s access to Eximills, discontinued offering Eximills to foreign banks and voluntarily disclosed the matter to relevant regulators, including OFAC and the Board of Governors of the Federal Reserve (the Fed).

According to the Fed’s Order, WFC cooperated with the Fed, including by ceasing and remediating the OFAC violations related to Eximills, and strengthening compliance with OFAC regulations. Nevertheless, the Fed noted that Wells Fargo’s oversight and risk management failures enabled the OFAC violations to occur, and issued a civil monetary penalty of \$67.8 million under the Federal Deposit Insurance Act (12 U.S.C. § 1818(i)(2)(B)) against WFC for the “unsafe or unsound practices” related to Eximills.

OFAC’s and the Fed’s enforcement actions against Wells Fargo are unusual in that they involve “facilitating” sanctions violations by non-U.S. persons where that facilitation arose from the deployment of an IT system.

While Wells Fargo did not, as a matter of law, inherit civil liability from Wachovia for its allegedly intentional sanctions-evading conduct, Wells Fargo was deemed liable for permitting Wachovia’s sanctions-evading IT system to continue, even unintentionally. OFAC and the Fed did not pursue enforcement related to Wachovia’s intentional provision of that IT system for the purpose of evading sanctions, possibly because the conduct was outside of the statute of limitations.

OFAC concluded that Wells Fargo’s senior management “should have reasonably known” that Bank A was using Wells Fargo’s IT platform to engage in transactions involving sanctioned jurisdictions and persons, especially considering that Wells Fargo compliance reviews raised potential concerns on numerous occasions.

OFAC did, however, consider it to be a mitigating factor that senior management at Wachovia and Wells Fargo did not appear to direct or have actual knowledge of the sanctions-implicating transactions, given the relationship between Wachovia and Bank A and that the provision of IT software to Bank A was helmed by a small legacy group within Wachovia.

## **Guidance for Compliance Personnel**

These enforcement actions illustrate the high cost of sanctions violations and—in our view—are bellwethers of increased federal enforcement activity in this area.

- 
- Companies should ensure that their U.S.-owned or hosted IT systems do not facilitate transactions in violation of U.S. sanctions or export controls.
  - Compliance personnel should conduct a robust assessment of their companies' IT systems to identify potential sanctions risks, and routinely audit those systems to ensure continued compliance.
  - Especially in connection with mergers and acquisitions transactions, compliance personnel should be mindful that sanctions violations might arise from legacy IT systems, and that a five-year lookback on an acquisition's transactions will not necessarily identify this risk.