

## **FINANCIAL FRAUD IN THE ELECTRONIC AGE**

*By Jeffrey E. Brandlin*

Big-time financial fraud artists – those who steal \$10 million to \$100 million or more, often from public companies – grow more inventive with each passing year. The electronic age gives them new ways to create and cover up their scams, showing how important it is for lenders and investors to keep their eyes peeled for mischief, and how difficult it is to uncover crime.

It was never easy to track financial fraud. In the past, the forensic accountant always knew to look for the “second set” of books – not the cooked books shown to outsiders, but rather the set containing the real data on the business operation. Even criminals cannot run a successful enterprise without good information, and Job One for the forensic accountant historically was always to lay hands on the second set of books.

Today, criminals use technology to create almost seamless electronic accounting records, making it increasingly difficult to surface their misdeeds without sophisticated equipment and investigative techniques. This is especially true when there exists an underlying business – often failing – onto which the criminal can graft the con.

In such circumstances, the object of the game is to deceive lenders into believing that the business is healthy, with growing revenues and quality assets. The criminals scam lenders into advancing funds against reported cash flow and assets, for example, inventory or receivables. To that end, the fraud artist creates a closed loop of phony business activity, generating financial statements that will hoodwink outsiders.

To demonstrate how this works, assume a company’s financials show \$500 million in revenues against \$450 million in cost of goods sold, plus operating expenses – in all appearances, a healthy company. Hidden in the numbers, however, is the real story: the company’s actual cash receipts from sales are \$370 million against \$400 million in expenses.

Clearly, this business is in trouble. So the principals, accustomed to comfortable lifestyles, create a loop of phony business activity starting with one or more bogus suppliers of inventory – in reality, sham entities controlled by the principals. They continue the loop by creating one or more bogus salespeople, and they close it with sales to bogus customers. Specifically, they concoct accounting entries showing the company buying inventory worth \$100 million from the bogus suppliers against which the bogus salespeople post sales of \$130 million to bogus customers.

**Teaming Integrity, Experience & Service  
For Superlative Results**

These are big numbers, but this is big-time fraud. The \$30 million spread between the cost of this bogus inventory and the sales it allegedly generates covers up the real losses of the underlying business. More important, it can fool a lender into seeing a bankable enterprise.

The problem for fraud artists, however, is to continue fooling their lenders year after year. To that end, fraud artists must invent bigger numbers every year – \$30 million in our example during the first year, more than that in the second, and so on. Put another way, by its very nature, fraud must accumulate, and this gets harder and harder to do as time passes, since fraud artists are often as lazy as they are greedy.

Clues to identifying such schemes include suspiciously round numbers, purchases from phony vendors that do not match up with those from real vendors of the same or similar items, or, sales posted by the phony salespeople that diverge substantially from those of real salespeople. For example, the books might show 1,000 units of a particular item purchased from one supplier at one price and 5,000 units of the identical item from another supplier – a bogus supplier controlled by the fraud artist – at twice the price. In one scheme I uncovered, the books showed 65,000 units of inventory purchased from one vendor and 64,000 units sold to one customer. The anomaly was that the company usually sold this item in 100-unit quantities.

Fraud like this means computers – usually no more than a handful per scam. The scheme may involve more than one criminal, but they do their data entry from a few terminals to which they alone have access, often in the offices of senior executives. Thus, for the forensic accountant, the key is to track down the right computers, just as, in the old days, the key was to lay hands on the second set of books.

Even so, it takes a high degree of skill and often a great deal of time to get to the truth of a fraud, not to mention patience. It costs money, too. But sometimes you get lucky. Criminals are commonly braggarts who cannot resist crowing if given the chance to talk. Choose the right moment to ask the right questions and some bad guys will tell you everything you need to know.

*Jeffrey E. Brandlin, CPA, is president of Brandlin & Associates, a Los Angeles-based forensic accounting firm specializing in financial due diligence, for lenders and investors, workout and bankruptcy consulting and litigation support. For more information, please visit [www.brandlin.com](http://www.brandlin.com).*

**Teaming Integrity, Experience & Service  
For Superlative Results**