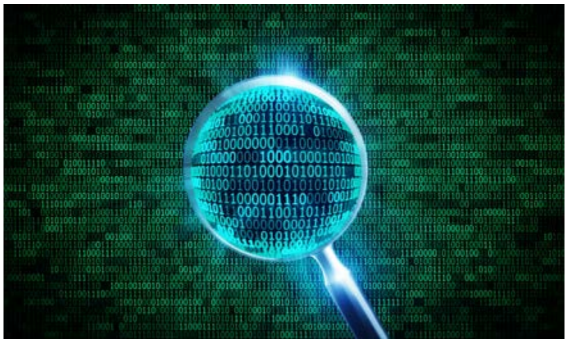
SIMON CONSULTING
Clarity. Integrity. Results.

602-279-7500 The Forensic Accounting Authority of the Southwest

# Fraudulent Manipulation of Bank Statements in Electronic Format

By Peter Davis, CPA, ABV, CFF, CIRA, CTP, CFE and Sara Beretta, CPA, CFE, CFI



Bank records are of particular interest and importance to forensic accountants and receivers, as they reflect an entity’s actual financial history. In fact, bank records can tell a powerful story. We identified bank statements in several of our investigations that were electronically manipulated to reflect deceptive and fraudulent statement entries. Both the descriptions and amounts were changed for electronic payments, such as wire transfers and debit card transactions reflected on statements.

In some cases, deposits were altered to reflect greater cash inflows, and the balances were manipulated such that they rolled forward, helping the manipulations go unnoticed.

Bank and credit card statements are often downloaded by accounting personnel from bank websites in PDF format, in lieu of receiving hard copies via mail. This practice is becoming increasingly common as companies are encouraged to go paperless. In some cases, we found that statements were manipulated using software that cracks open PDF files and provides editing tools that were used to change amounts, dates, and descriptions of various transactions. The files were then converted back to PDF format.

Today, bank records can be easily manipulated using Adobe Acrobat Pro software, which doesn’t require converting the file to a different format.  For example, imagine a case of employee embezzlement, in which an employee uses a company credit card for personal purposes.  If the employee has access to the electronic statements, it would be incredibly easy to change the payee name from a department store to a less questionable vendor, such as an office supply store.

Inevitably, all PDF files are editable. Even if the original PDF file is scanned as an image in bitmap format, a process known as Optical Character Recognition (OCR) allows users to convert the PDF into text format. Adobe Acrobat contains an OCR feature, and there is other software available on the internet. Even PDF files that are not in text format can still be edited through other means. Techniques such as using screen capture software to take an image of the document and then editing and resaving it can be used to change an electronic file.

Some financial institutions apply security features to PDF files, which can help to prevent manipulation. In our experience, this occurs most often with investment accounts. In Adobe Acrobat Pro, you can check whether security features have been applied to a PDF file to determine if the document is subject to manipulation. These security features can only be removed if you know the password used to enable them. However, in our experience, most banks don't apply these simple security features to electronic statements.

The most secure PDF files can restrict users from changing a document, combining multiple files, extracting pages, copying text, and even printing the files. Although this security feature is almost never used, one might question why a financial institution would want to prevent users from printing out statements. Someone with access to printed statements could simply scan them back into PDF format and convert them into text, which essentially washes away all security features applied to the original electronic file. The creator of the PDF can implement password protection, but ultimately, this protection can be broken.

Changes made to bank statements are virtually impossible to identify without having a copy of the original bank statement to compare them to. Forensic accountants and receivers should exercise caution when relying on bank and credit card statements in PDF format, unless they come directly from the financial institution. Specifically, there are a few things to look out for with regard to statements received from other sources:

(1) Look for slight differences in font types and sizes. Some banks use more obscure fonts that are difficult for basic OCR software to match.
(2) Look for statements that appear to have been scanned but have been converted to text format, as such documents reflect the potential for manipulation.
(3) Match ending balances from prior statements to beginning balances of subsequent statements. It can be difficult to carry on the manipulation without error for an extended period of time.
(4) Look for excessive bank fees, as such fees might be indicative of overdraws despite an apparent positive cash balance.

The ease of electronic manipulation teaches a valuable lesson. We must remember to exercise caution, and remain on heightened alert of fraudulent schemes in the analysis of bank records.