USING DATA ANALYTICS TO DETECT DISBURSEMENTS FRAUD

By William W. Acuff, CPA, CFF, CFE, CIA, CGMA, and Thomas A. Gavin, DBA, CPA, CGMA

Regardless of industry, disbursement fraud schemes are among the most pervasive types of fraud. Many perpetrators conceal their disbursement schemes using rather simple methods because they perceive no one is looking. Data analytics software provides methods to identify transactions that represent potential disbursement fraud.

Case: An Unsophisticated Fraud

The director of accounts payable for a large manufacturing company continued making payments on a vendor's expired contract, except she changed the vendor's bank routing number in the vendor master file to the same direct deposit bank routing number she had provided to the payroll department.

Over a five-year period, she wired over $650,000 to her personal bank account. This fraud scheme may have continued for many years if it had not been for an anonymous tip to the company's reporting hotline after she bragged about being able to take money from her employer.

Her fraud scheme was one of the most common types of disbursement fraud schemes: a type of billing scheme that makes use of an existing vendor (Table 1). Usually, disbursement fraud schemes are simple to perpetrate; however, concealment of the fraud in the books and records of an organization can range from simple to more sophisticated methods of concealment.

Table 1 - Fraudulent Disbursement Schemes [1]	
Billing Schemes -Shell Company -Non-Accomplish Vendor -Personal Purchases	A fraudulent disbursement scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for personal purchases.
Payroll Schemes -Ghost Employee -Falsified Wages -Commission Schemes	A fraudulent disbursement scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation.
Expense Reimbursement Schemes -Mischaracterized Expenses -Overstated Expenses -Fictitious Expenses -Multiple Reimbursements	A fraudulent disbursement scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses.
Check Tampering -Forged Maker -Forged Endorsement -Altered Payee -Authorized Maker	A fraudulent disbursement scheme in which a person steals his or her employer's funds by intercepting, forging or altering a check drawn on one of the organization's bank accounts.
Register Disbursements -False Voids -False Refunds	A fraudulent disbursement scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash.

Concealment is the Key to Detection

Fraud schemes differ from robbery; in the former, the perpetrator employs the mask of deception to commit the offense. The deception or concealment generally manifests itself to the fraud analyst in the form of anomalies (red flags) within a transactional data file. Knowing and being able to recognize these red flags is the key to developing detection strategies.

In the range of simple to complex fraud schemes, the billing scheme described above would be considered a simple or lower-level concealment because the perpetrator used information that could be detected by directly matching identifying data points, i.e., her bank routing number to the payment transaction in question. Alternatively, in a higher-level concealment, a payment could be made to the account of a specially created shell company at a bank not known to be used by either the organization or the perpetrator.

Proactive Fraud Detection

People commit fraud because they perceive an opportunity exists to commit and conceal the fraud without detection. Proactive data monitoring/analysis has been found to be one of the most effective anti-fraud controls. This is because the threat of likely detection is one of the most powerful fraud prevention techniques. It all but eliminates the fraudster's perceived opportunity.[1]

Preventative controls alone are not effective in managing the business risk of fraud, as there will always be people who are motivated to commit fraud.[2] Each organization should perform a relevant risk assessment, adopt and implement appropriate preventive control policies and procedures, and then monitor on a timely basis. Morphing from potential to real perpetrator is accelerated when those responsible for entity assets and preventive controls are not effectively managing business risks.

A proactive detection program increases the perception that fraud will be detected. The reasonable cost of such efforts can significantly mitigate emotional and monetary losses. As the saying goes, "There are no small frauds, just large ones detected early."[3] It has been reported that 58 percent of defrauded organizations recover none of their losses, while only 14 percent are made whole after being victimized.[1]

Returning to our case, limiting access to the vendor master file is one of the most effective preventive controls for billing schemes; this control was not present in the victim organization. A proactive detection program that includes the test described above would have most likely detected this unsophisticated concealment.

Ways to Use Data Analytics in Disbursements Fraud Detection

Data analytics can be used in two ways to detect disbursements fraud: 1) analyzing entire populations of transactional data to look for anomalies and/or 2) analyzing transactions for indicators of known fraud risks. Both techniques should be used when proactively attempting to detect fraud in a transactional database.

Many professionals now use data analytics software to detect fraud because of its ability to profile and interrogate 100 percent of a transactional dataset to identify fraud's anomalies and red flags; that is to say, identifying anomalous patterns (numeric, time, geographic and naming fields) within the dataset. Sampling software's functionality and ease of use is not up to the task at hand.

The functionality of data analytics software incorporates many user-friendly tests and techniques, such as fuzzy matching and digital tests like Benford's Law. The software lends itself to test development and the refinement of pre-written tests, and it provides the ability to automate test on a continuing basis. >

Table 2 - Nigrini Cycle [4]	
High Level Overview Tests	
Data Profile	Provides insight into distribution of numbers.
Data Histogram	Counts of amounts in various intervals.
Periodic Graph	Distribution of numbers across time.
Benford's Law-based Tests	
First-two Digits	More focused than first digit and second digit tests and identifies abnormal duplications.
Second Order Test	Based on the digits of the differences between amounts that have been sorted from smallest to largest.
Summation Test	Looks for excessively large numbers in the data.
Number Duplication	Identifies which specific numbers causing spikes on the first-order test.
Last-two Digits	Powerful for number invention.
Advanced Tests	
Largest Subsets	Subset of a group of records that have something in common, focusing on subsets that are highly inflated.
Same Same Different	Identifies transactions that are linked to two different subsets.
Relative Size Factor	Identifies subsets where the largest amount is out of line with the other amounts.

Analyze Entire Populations of Transactional Data to Look for Anomalies

The Nigrini Cycle, introduced several years ago, consists of a series of eight high-level dataset tests that analyze data in a single field (Table 2). The eightfold dataset tests consist of three high-level overview tests (data profile, data histogram and periodic graph) and five Benford's Law-based tests: first-two digits, second order, summation, number duplication and last-two digits. These tests provide valuable insights into the internal diagnostics of the dataset.[4]

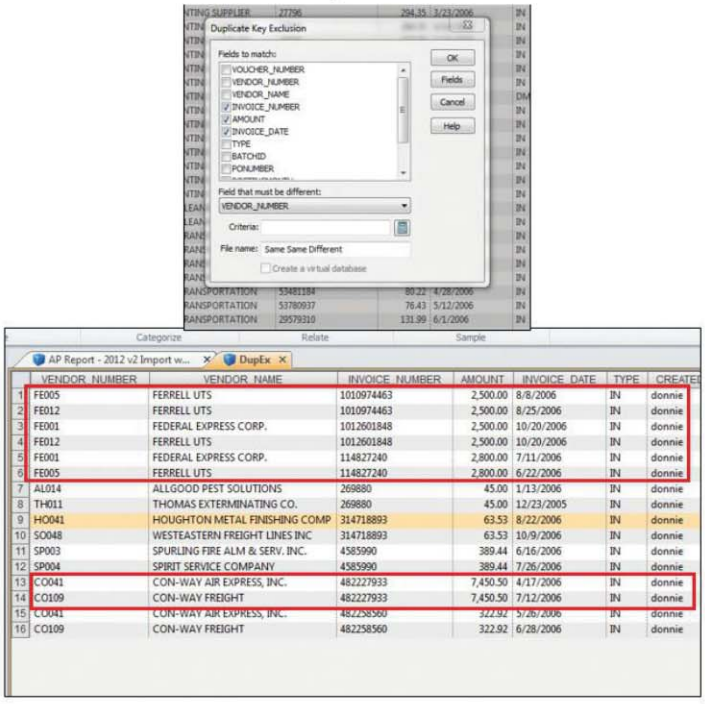
The tests' creator also suggests running advanced tests, as these powerful techniques employ more than one field of data and consist of largest subsets, same same different and relative size factor tests (Table 2). For example, the analyst may perform the same same different test on a paid invoice file when looking for transactions linked to two different subsets. In a duplicate payments scheme, achieved by a simple concealment, the fraudster may use the same invoice number, amount and invoice date but post the invoices to two different vendors. Figure 1 shows the results of running the same same different test on a paid invoice file to identify potential fraudulent payment transactions.

Analyze Transactions for Indicators of Known Fraud Risks

Every organization should assess fraud risk or perceived opportunities to commit and conceal fraud. The fraud risk assessment should be based on specific fraud schemes inherent within each organization. The fraud analyst should develop scenarios based on both the controls and processes in place within each organization and how the fraud schemes could be concealed.

Once specific fraud schemes and their various red flags of concealment are identified, then tests should be selected or developed to identify transactions displaying these indicators. For example, the concealment method for several types of inherent fraud schemes produces the red flag of duplicate payments appearing in the books and records of an

Figure 1



	VENDOR_NUMBER	VENDOR_NAME	INVOICE_NUMBER	AMOUNT	INVOICE_DATE	TYPE	CREATE
1	FE005	FERRELL UTS	1010974463	2,500.00	8/8/2006	IN	donnie
2	FE012	FERRELL UTS	1010974463	2,500.00	8/25/2006	IN	donnie
3	FE001	FEDERAL EXPRESS CORP.	1012601848	2,500.00	10/20/2006	IN	donnie
4	FE012	FERRELL UTS	1012601848	2,500.00	10/20/2006	IN	donnie
5	FE001	FEDERAL EXPRESS CORP.	114827240	2,800.00	7/11/2006	IN	donnie
6	FE005	FERRELL UTS	114827240	2,800.00	6/22/2006	IN	donnie
7	AL014	ALLGOOD PEST SOLUTIONS	269880	45.00	1/13/2006	IN	donnie
8	TH011	THOMAS EXTERMINATING CO.	269880	45.00	12/23/2005	IN	donnie
9	HO041	HOUGHTON METAL FINISHING COMP	314718893	63.53	8/22/2006	IN	donnie
10	SO048	WESTEASTERN FREIGHT LINES INC	314718893	63.53	10/9/2006	IN	donnie
11	SP003	SPURLING FIRE ALM & SERV. INC.	4585990	389.44	6/16/2006	IN	donnie
12	SP004	SPIRIT SERVICE COMPANY	4585990	389.44	7/26/2006	IN	donnie
13	CO041	CON-WAY AIR EXPRESS, INC.	482227933	7,450.50	4/17/2006	IN	donnie
14	CO109	CON-WAY FREIGHT	482227933	7,450.50	7/12/2006	IN	donnie
15	CO041	CON-WAY AIR EXPRESS, INC.	482258560	322.92	5/26/2006	IN	donnie
16	CO109	CON-WAY FREIGHT	482258560	322.92	6/28/2006	IN	donnie

Note: Same same different test where invoice number, amount and date are the same with different vendor number, shows four duplicate payments within the dataset.

organization. As discussed above, in testing for duplicate payments, the same same different test could detect simple concealments. However, this test would not be effective if the fraudster changed the invoice number, amount or date; more advance tests using fuzzy logic to match data points would be required.

Given known fraud risks, there are many tests to detect disbursements fraud. Common data analytics applications to detect fraud based on known fraud risks include:

- Identification of employee/vendor relationships looking for matches between and within the vendor master and employee master files.
- Indicators of fictitious vendors such as incomplete information in the vendor master.
- Analysis of purchasing card activity for indications of personal use.
- Indicators of ghost employees, terminated employees or invalid social security numbers.
- Trend analysis of vendor payments and duplicate payments testing.
- Trend analysis of payroll hours and earnings and matches between the employee master and the payroll disbursements file.

Conclusion

Fraudsters employ various levels of sophistication to conceal their schemes. Many of these schemes, especially low-level concealments, could be detected if a viable detection program were in place. When beginning a detection program using data analytics, identify and define specific fraud risks to be tested. Start with relatively simple tests, then add more complex analysis as necessary to address the issues at hand and to build a library of specific tests that can then be used in recurring audit engagements or continuous auditing.

RESOURCES

[1] *2014 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse*, published May 2014 by the Association of Certified Fraud Examiners.

[2] *Managing the Business Risk of Fraud: A Practical Guide*, published June 2008 by the Institute of Internal Auditors, the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

[3] *Fraud Magazine*, Association of Certified Fraud Examiners, "7 Keys to an Effective Fraud-Fighting Career," published January 2015 by Steve Albrecht, Ph.D., CFE, CPA.

[4] *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*, published 2011 by Mark J. Nigrini, Ph.D.; table developed by William Acuff.

ABOUT THE AUTHORS

WILLIAM W. ACUFF, CPA, CFE, CIA, CGMA, is managing partner of Forensic and Fraud Investigations PLLC. He has 30 years of public accounting experience using data analysis software in investigations and fraud audits. Acuff will be speaking at this year's Forensic & Valuation Services Conference on this topic. He can be reached at *wwacpa@epbfi.com*.

THOMAS A. GAVIN, DBA, CPA, CGMA, is CEO of Abacus-AT-e2, LLC, a human resource and educational services firm, and Decosimo Professor of Accounting Emeritus within the University of Tennessee system. He can be reached at *aqgavin@epbfi.com*.