



**McGOVERN & GREENE** LLP  
CPAs & Forensic Accountants

**McGovern & Greene LLP** is a CPA/forensic accounting and consulting firm with office locations in: Chicago, IL ; Las Vegas, NV; and Atlanta, GA. The firm is comprised of specialists in fraud examination, forensic accounting, computer forensics, and litigation services. We are regularly retained by major corporations, law firms, government and law enforcement agencies when fraud is suspected.

**ELFF**

ELFF is M&G's "ELECTronic Fraud Fighting" tool that encompasses a comprehensive suite of data mining services designed to detect procurement and disbursement frauds and errors that may exist in your organization.

ELFF's algorithms identify errors and inefficiencies in your accounts payable system:

- Duplicate payments
- Multiple vendor entries
- Missed discounts

ELFF's algorithms also help you to identify the major procurement and disbursement transactions associated with fraud:

- Non-existent vendors
- Fraudulent invoices associated with legitimate vendors
- Duplicate payments
- Employees as vendors
- Pricing variances

**INVESTIGATION AND AUDIT**

After running ELFF you should have an excellent place to start with any audit or investigation. Should you feel your company lacks the investigative/audit skills and staff to properly proceed, McGovern & Greene LLP can assist you. Our trained fraud examiners, forensic accountants and financial investigators routinely investigate a multitude of employee and vendor frauds, either independently or supplementing your own entity's department.

**ELFF**



**ELECTRONIC  
FRAUD  
FIGHTING  
PROGRAM**

ELFF was created by  
**Christy Warner** and  
**Craig L. Greene, CFE,**  
CPA/CFE, MSJ.

**Christy Warner** is a mathematician, statistician and database design expert who has worked in data mining for over 14 years, unearthing major fraud cases.

**Craig L. Greene** is a Certified Fraud Examiner and Certified Public Accountant, Certified in Financial Forensics. He has worked as an auditor and forensic accountant for over 35 years, investigating complex fraud schemes and recovering millions of dollars for his clients.

**McGOVERN &  
GREENE** LLP  
CPAs & Forensic  
Accountants



Contact **Craig Greene** for  
full pricing information at  
one of our offices or Email:  
[craig.greene@mcgoverngreene.com](mailto:craig.greene@mcgoverngreene.com)

**Las Vegas**

2831 St. Rose Parkway • Suite 285  
Henderson NV • 89252  
Ph: 702.818.1168

**Chicago**

200 W. Jackson Blvd. • Suite 2325  
Chicago IL • 60606  
Ph: 312.692.1000

**Atlanta**

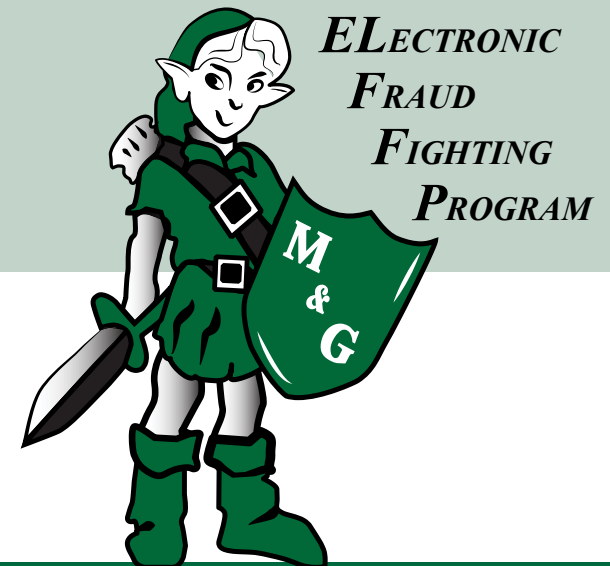
1205 Johnson Ferry Rd • Suite 136-508  
Marietta GA • 30068  
Ph: 770.362.2008



**McGOVERN & GREENE** LLP  
CPAs & Forensic Accountants

**DATA MINING  
SERVICES**

**ELFF**



**ELECTRONIC  
FRAUD  
FIGHTING  
PROGRAM**

**ELFF may be applied to identify all of the following situations:**

## **ERRORS AND INEFFICIENCIES**

### **Missed Discount Detection and Recovery**

Negotiated payment terms that should result in a discount are often missed by Accounts Payable systems. ELFF searches your accounts payable files for missed discounts by comparing the payment terms with the invoice date, check date, invoice amount and discount-taken fields. This can help to quantify the additional cost to your organization from both situations where the discount terms were met, but the discount was not taken; and also the total discounts that could have been taken had payment been more prompt. This can help you identify a significant savings to your organization.

### **Erroneous Overpayment Detection and Recovery**

ELFF can reconcile your purchase order file with your accounts payable file to detect pricing errors and any overpayments that may have occurred for products that were never received. Your organization can then seek to recover the overpayments from the vendor.

### **Duplicate Payment & Vendor Detection**

ELFF's duplicate payment detection uses a comprehensive set of algorithms. While most duplicate payment identification plans employ 3 or 4 patterns, ELFF uses 10 intelligent algorithms and incorporates duplicate vendor logic to capture the maximum number of duplicate invoices and vendors. The search for duplicate vendors utilizes five different search criteria: 1) Address, 2) Tax ID, 3) Bank Routing Number, 4) Name, and 5) Phone Number, and uses fuzzy logic to identify similar but not exact matches.

Multiple vendor listings for the same entity can lead to issues with improper payments, including allowing duplicate payments. By identifying these situations you can improve the efficiency of your accounts payable department. In addition, duplicate vendors represent a fraud risk, allowing your employees to include fraudulent invoices in your system. Using ELFF to identify these situations can improve not just your operating efficiency, but also your system of internal control.

## **IDENTIFYING FICTITIOUS/ FRAUDULENT VENDORS**

### **Vendor/Employee Cross Check**

Too often frauds involving procurement/payables involve a company's own employees. ELFF compares your vendor and employee data for similarities in: 1) Address, 2) Tax ID, 3) Bank Routing Number, and 4) Phone Number. This may identify an undisclosed relationship between one of your employees and an apparent vendor.

### **Employee Earnings Analysis**

Analyzing your employees' earnings and withholding can provide significant indicators of fraudulent behavior. ELFF analyzes the withholding and payroll data and flags the outliers. Those with minimal or no withholding or deductions for benefits may be ghost employees. Those who have higher than usual withholding may be trying to compensate for their illicit income. It is surprising the number of employees that will steal from their employers, but don't want to risk running afoul of the IRS.

### **Payments Dated on a Weekend**

ELFF identifies any check, electronic fund transfer or other disbursement dated on a Saturday or Sunday, as these are unusual in the business world.

### **Vendors Consistently Paid Quickly**

If a vendor is consistently being paid before or on the invoice due date, it may be indicative of a fictitious vendor or fraudulent corruption scheme. In both cases one of your employees would be involved and eager to not only receive the payment, but close out the invoice so it may go unnoticed. ELFF calculates the difference between the invoice date and check date, and ranks the vendors by speed of payment so you may easily identify the most likely vendors of concern.

### **Suspicious Vendor Data**

The fact that a vendor uses a PO Box or has a mail drop address does not on its own indicate that the vendor may be fictitious. However, a report pinpointing these vendors can then be compared to the results of other reports. The more often a vendor appears, the greater the likelihood that the vendor may be fictitious or your transactions with it fraudulent. Because it is not always obvious that a vendor uses a mail drop address, ELFF incorporates a function that compares the vendor address with mail drop addresses to identify these vendors.

## **IDENTIFYING FRAUDULENT INVOICES**

### **Rounded Amount Invoices**

Invoices in round amounts or without pennies in the total may be indicative of fraudulent invoices. ELFF identifies these invoices and ranks them by the vendors who have the highest percentage of relevant activity. For example, a vendor issuing 100% of their invoices without pennies would appear first on the list.

### **Invoices Just Below Approval Amounts**

Fraudsters that know your approval limits will often keep their fraudulent invoices right below this amount so as to avoid additional scrutiny.

ELFF's proprietary algorithms identify invoices that fall up to 3% below the approval amount. It also ranks vendors according to the percentage of their invoices falling just below the approval amount.

### **Significant Change in Volume or Value of a Vendor's Invoices**

Purchasing from vendors usually remains relatively consistent for the number and total cost of invoices per month. ELFF analyzes the invoices by vendor and identifies unusual changes in volume and total cost, either up or down. A significant increase in volume or total dollars spent could indicate that fraudulent invoices are being attributed to that vendor. It could also mean that one of your employees has accepted a kickback of some sort to increase purchasing through that vendor. A decrease in vendor invoice volume or cost could indicate that a fraudster has gotten spooked and stopped including fraudulent invoices so as to avoid detection.

### **Sequentially Numbered Invoices**

Invoices from a vendor are not likely to be consistently sequential unless you are their only customer. However, sequential invoices are likely for orders taken around the same time. ELFF's algorithms analyze the frequency of sequential invoice numbers and rank the vendors by the frequency of this occurrence. The most frequent vendors may be fictitious or fraudulent vendors and bear investigating.

### **Summarizing Results**

ELFF summarizes the suspected transactions and vendors based on the results of all reports, ranking them by likelihood of fraudulent activity. This ranking helps to focus your audits and investigations on the truly deviant transactions and/or vendors.