



**Decide with Confidence**

# Shifting the Fraud Paradigm: From 'Pay and Chase' to Prevention

*How government agencies can stop fraud before it even begins*

WHITE PAPER

*By Tom Marsden*



**Decide with Confidence**

## Table of Contents

Section I: Executive Summary .....	2
Section II: Transforming Government's Fraud Prevention Practices .....	3
Section III: The 5 Cs of Fraud Prevention.....	4
Section IV: Case Studies in Fraud Prevention .....	6
Section V: Trends in Government Fraud Prevention.....	12
Section VI: Conclusion .....	13



## Section I: Executive Summary

### **The Five Cs of Fraud Protection**

**Confirmation:** *Does the person or entity truly exist?*

**Condition:** *Is the business and/or its executives active?*

**Consistency:** *Are stated facts consistent with other sources of information?*

**Character:** *Are there any past issues that could impose risks on the current or a future transaction?*

**Continuity:** *Has the current operational status changed and is it posing new risks?*

Fraud prevention goes hand in hand with good government. This connection, while never in dispute, is highlighted by current efforts to strengthen government accountability and performance. When offering guidance for implementing the American Recovery and Investment Act, White House Budget Director Peter Orszag emphasized the need to combat fraud more than a dozen times in a memo to federal leaders, saying agencies must put in place “defined strategies to prevent or timely detect waste, fraud, or abuse.”<sup>1</sup> In other initiatives as well, the White House is pushing agencies to improve internal controls aimed at preventing fraud and preserving program integrity. “Far too often, [government] spending is plagued by massive cost overruns, outright fraud, and the absence of oversight and accountability,” President Barack Obama said when releasing the administration’s plan for improving government contracting practices. “It’s time for this waste and inefficiency to end.”<sup>2</sup>

Few would question the need for improved fraud prevention, but the question for many is how to begin. In this regard, commercial best practices for lender and credit management provide a foundation for building the tools and processes that can help government agencies significantly reduce fraud. In particular, an approach known as the five Cs of fraud prevention has been adopted with overwhelming success by a number of federal agencies. The five Cs approach provides agency leaders with a strategic framework that can guide their efforts to incorporate fraud prevention activities within existing organizational processes, IT systems, and structures. This approach also enables agencies to take advantage of third-party vendors that can provide large databases of information and expertise to help agencies put into place effective fraud prevention practices.

Fraud prevention ensures that grants, assistance and other payments reach the hands of the businesses and people who need them. Moreover, with effective mechanisms in place, government employees can spend more time focusing on their agency’s mission and less time trying to chase down fraud and abuse. An ounce of prevention is worth a pound of investigation.

---

<sup>1</sup> “Memorandum for the Heads of Departments and Agencies,” February 18, 2009, p. 51.

<sup>2</sup> “Remarks by the President on Procurement,” March 4, 2009.



Decide with Confidence

## Section II: Transforming Government's Fraud Prevention Practices

The need for fraud prevention is not new. Federal and state governments lose tens of billions of dollars every year to fraud and improper payments, as revealed in numerous reports by the Government Accountability Office and agency Inspector General offices.<sup>3</sup> What is new, however, is the current Administration's extraordinary emphasis on rooting out waste and fraud in government contracting, grants, loans, medical reimbursements and all federal programs. President Obama has made clear his intent to use new information technologies and interactive media to transform government by promoting transparency, accountability, oversight and program integrity. Among his recent initiatives, the president appointed Interior Department Inspector General Earl Devaney as head of the new Recovery Act Transparency and Accountability Board. In this role, Devaney will serve as a watchdog to guard against fraud in the \$787 billion stimulus package. Devaney, who estimates that as much as 7 percent of spending is often lost to fraud, said he is eschewing traditional approaches that focus on catching scammers and criminals after they've taken government money. "The approach here has to be at the front end of the pipeline," he said.<sup>4</sup>

*"We have to get in on the front end and try to prevent waster, fraud and abuse before it happens."*

*Earl Devaney  
Chairman  
Recovery Act Transparency and  
Accountability Board*

By requiring agencies to carefully track and account for their spending, the Recovery Act provides both a mandate and opportunity for agencies to begin implementing effective fraud prevention practices. Agencies welcome this chance to strengthen spending controls and demonstrate their commitment to effective government, but few have the experience or resources required for a comprehensive fraud prevention program. Fraud prevention is not a

---

<sup>3</sup> For recent examples, see "Medicare: Improvements Needed to Address Improper Payments in Home Health" (GAO-09-185; February 2009); "Emergency Management: Actions to Implement Select Provisions Post-Katrina Emergency Management Reform Act" (GAO-09-433T; March 17, 2009); and "Federal Farm Programs: USDA Needs to Strengthen Controls to Prevent Payment to Individuals Who Exceed Income Eligibility Limits" (GAO-09-67; October 2008).

<sup>4</sup> "Transcript: Earl Devaney," *Wall Street Journal*, March 8, 2009. Devaney's assertion that as much as 7 percent of funding is lost to fraud may seem high, but we have found instances where the percentage is even larger. The GAO, for example, estimated that during the first 18 months following Hurricane Katrina, the government made about 16 percent—or \$1 billion—in improper and potentially fraudulent payments to applicants who used invalid information to apply for disaster assistance. "Actions to Implement Select Provisions Post-Katrina Emergency Management Reform Act," p. 28.



**Decide with Confidence**

core mission capability, even among agencies that have strong auditing capabilities. And so agencies face many challenges implementing this new federal mandate. Agency leaders ask: Do our databases contain the necessary information to effectively track contractors, grant recipients, Medicare and Medicaid providers, or other recipients our agency's funds? How do we set up the right processes for uncovering potential fraud and abuse, and then create the right procedures controlling fraud when we find it? Can we do it with existing staff and resources?

## Section III: The Five Cs of Fraud Prevention

The five Cs of fraud prevention offer insight and guidance on how to address these important questions. Adapted from commercial best practices for credit management, the five Cs approach is built upon the concept of due diligence. The key to fraud prevention for public and private sector organizations, due diligence is defined as the care a prudent person would take in the examination of risks associated with a business transaction. In the case of the government, the "business transaction" might be a contract award to a large aerospace company, a small business loan to an urban business, a research grant to a university scientist, Medicare reimbursement to a hospital, or a disability check to a military veteran. All of these are worthwhile expenditures. The task facing government agencies that oversee these transactions is threefold. They must ensure that: 1) the organizations or persons receiving government funds are who they claim to be; 2) the money is spent for its intended purpose; and 3) the government receives the agreed-upon product or service.

While every agency conducts some measure of due diligence in this regard, the principles underlying the five Cs of fraud prevention provide a conceptual framework for building systematic, vigorous and comprehensive due diligence into an agency's existing controls and information systems. The five Cs of fraud prevention are:

- **Confirmation.** Does the person or entity truly exist? A check of databases might reveal that a particular business isn't registered to operate in the state, or that its purported address doesn't exist, or that an applicant's Social Security number belongs to a deceased person.



**Decide with Confidence**

- **Condition.** Is the business and/or its executives active? Although you have confirmed that the business exists, you discover that it has no telephone number, fax number, Website, or e-mail address. Or perhaps its business license expired three years ago and hasn't been renewed.
- **Consistency.** Are stated facts consistent with other sources of information? After you confirm that the business exists and is operating, you discover that the company president also runs 15 other businesses registered at the same address—a residential dwelling with a home telephone number.
- **Character.** Are there any past issues that could impose risks on the current or a future transaction? Criminal and background checks might reveal a past that includes bankrupt businesses, complaints with the Better Business Bureau, or arrests for criminal fraud.
- **Continuity.** Has the current operational status changed and is it posing new risks? Even after your contracts are signed and the contractors are performing, you want a system that continually monitors contractors for events that indicate potential trouble, such as a Chapter 11 bankruptcy filing or SEC charges for stock irregularities.

When banks and credit card companies issue credit, they have access to a variety of public records to evaluate—that is, conduct due diligence on—individuals and businesses. In addition to using information provided by borrowers, banks can check credit records, criminal records, business registration records, fraud repositories, postal databases and a variety of public records. Although no method is 100 percent fool proof, due diligence is much less expensive than trying to recover funds resulting from fraud and other problems. The mortgage crisis that helped trigger the current worldwide recession resulted in large part because banks, insurance companies and other institutions abandoned traditional due-diligence procedures for managing risk, such as confirming a borrower's credit history, character, collateral, or ability to make payments.<sup>5</sup>

---

<sup>5</sup> The five Cs of commercial credit management are: 1) Capacity of the borrower to repay to the loan, such as cash flow and payment history; 2) Capital that the individual or business has invested—and will lose—if the project fails; 3) Collateral the borrower offers to cover loan payments; 4) Conditions or intended purpose of the loan; and 5) Character or trustworthiness of the individual or business receiving the loan.



**Decide with Confidence**

Although government agencies possess large stores of information about contractors and other entities that receive government funds, agencies can bolster their fraud prevention capabilities through information and due-diligence services offered by private-sector companies. Most of these companies are familiar names in the area of consumer and business information, such as Dun & Bradstreet, Thomson Reuters and LexisNexis. With their vast databases, they can help agencies locate individuals who owe child support or businesses that have failed to pay penalties or taxes. They can authenticate individuals and businesses that apply for government licenses or assistance, help law enforcement agencies track criminal enterprises, confirm the legitimacy and viability of government contractors, and screen healthcare providers for government medical insurance programs.

It is important to note that when conducting due diligence, there typically isn't just one piece of information—one “red flag” or anomaly—that confirms significant risk of fraud. Rather, it's a pattern or accumulation of red flags, such as a previous filing of bankruptcy, a rapid turnover in executive leadership, no business license or no record of paying state income taxes. None is decisive on its own, but taken together they create a picture of risk. Consequently, the ability to prevent fraud rests heavily on having access to updated business and consumer information, either in-house or maintained by third parties, which can provide a comprehensive view of entities that apply to receive public funds. One red flag signals potential risk. Multiple red flags confirm fraud risk.

## Section IV: Case Studies in Fraud Prevention

How would expanded access to business and consumer information strengthen fraud prevention? Listed below are case studies examining known instances of fraud that were perpetrated against government agencies. Each case looks at the fraud in the context of the five Cs, showing how publicly available information would have made detection and prevention much easier.



Decide with Confidence

---

## Confirmation: *Does the person or entity truly exist?*

### Confirmation Red Flags

- *No information confirming that the individual or business exists*
- *No confirmation of current business operating status*
- *Discrepancies with start date, business licensing, and tax registration*
- *Business is located at a residential address*
- *Address information is inconsistent with public records*
- *Business location not equipped to conduct stated operations*
- *Different businesses share common names, telephone numbers and addresses*
- *Executive background is characterized by risk, such as convictions for fraud or theft*
- *In business for years, but there are no B2B payment experiences (e.g., no telephone, office supplies, or electricity bills, etc.)*

**Company:** Custer Battles

**Location:** 55 Hammerlund Way, Middleton, R.I.

**Executives:** Scott Custer, Mike Battles, and Rob Roy Trumble

**Problem:** Custer Battles was banned from Defense Department contracting in 2004 and subsequently found liable for fraudulently billing the government for its work in Iraq. Nevertheless, company executives, Scott Custer, Mike Battles, and Rob Roy Trumble, formed new companies and continued winning work in Iraq.

**The Five Cs analysis:** A query of business records shows that three new businesses—CusterBattles Levant, Tarheel Training, and Emergent Business Services—began operating from the same address, 55 Hammerlund Way in Middleton, R.I. An executive query into employer records shows that Rob Trumble, a former executive with CusterBattles, runs all three companies. The executive query also connects both Trumble and Custer to the 55 Hammerlund Way address.

**Why is this significant?** A relatively simple search into known information about the business and its executives would have alerted Pentagon officials that executives of the banned company were still trying to obtain military contracts through new companies that they had created.



Decide with Confidence

---

## Condition: *Is the business and/or its executives active?*

### Condition Red Flags

- *No confirmation of current business operating status*
- *Little to no information on executive*
- *No indication of accounts or customers*
- *Business location not equipped to conduct stated operations*
- *Payment experiences do not match the standards industry B2B profile for comparable firms (based on Standard Industrial Classification (SIC))*
- *No record of line of credit or secured financing extended to the business*
- *Questionable trade experiences or documentary evidence*

**Company:** Bass Orthopedic

**Location:** Two rented mailboxes at Eglin Air Force Base, Florida

**Executive:** Unknown

**Problem:** Bass Orthopedic was a phantom company that received \$2.1 million in fraudulent Medicare claims. None of the doctors or patients listed by Bass Orthopedic in its claims had any dealings with the company. By the time a judge ordered the company's assets frozen, both the money and the owner had disappeared.

**The Five Cs analysis:** A business query using business registration, postal records and telephone directories reveals that Bass Orthopedic has no physical address and that no one answers the phone at the number listed. An executive query using credit records and open sources fails to find any information about an owner, including a name.

**Why is this significant?** A simple search into Bass Orthopedic would have uncovered several red flags alerting government authorities to a potential risk of fraud—before any claims were paid.



---

## Consistency: *Are stated facts consistent with other sources of information?*

### Consistency Red Flags

- *Discrepancies with start date, business licensing, and tax registration*
- *Business is located at a residential address*
- *Address information is inconsistent with public records*
- *One person operation (only the executive is listed as an employee) operating a million dollar-plus business*
- *In business for years, but there are no B2B payment experiences (e.g., no telephone, office supplies, or electricity bills, etc.)*

**Company:** Infinite Pills

**Location:** Sellersville, Pennsylvania

**Executive:** Robert Brehm

**Problem:** After Infinite Pills applied for a Certificate of Registration to operate as a distributor of controlled substances, the Drug Enforcement Administration conducted a routine on-site pre-registration inspection of the proposed business. The inspection found that the registered location was a private, residential townhouse owned by the applicant's mother. The owner, Robert Brehm, had no working experience or knowledge of pharmaceuticals. In addition, Brehm did not have potential customers, nor had he developed a recordkeeping or invoicing system for his business. As a result of the on-site inspection, the DEA denied Infinite Pills' application as a distributor.

**The Five Cs analysis:** A query of business registration and postal records show that the location and phone number were residential, not commercial. A query of criminal records and open sources reveal that Brehm is 20 years old and has no experience handling controlled substances. In addition, the Pennsylvania Department of Health has a complaint alleging that Brehm was "stockpiling nitrous oxide," and he has a police record.

**Why is this significant?** A search of available record may have uncovered the necessary information to deny Infinite Pills a license to distribute controlled substances. Such searches are much more cost-effective than sending agents long distances to conduct on-site inspections. Using this approach would not only enable DEA to review applications more quickly, but it also would provide an easy means to continuously monitor companies. Most importantly, it would free up agents to work on DEA's most critical cases.



Decide with Confidence

---

**Character:** *Are there any past issues that could impose risks on the current or a future transaction?*

**Character Red Flags**

- *Executive background is characterized by risk, such as convictions for fraud or theft*
- *Business principal/officer linked to other confirmed higher risk or failed businesses*
- *Executive linked to multiple similar businesses, including several inactive ones in operation for a short time*
- *Credit references provided by previously confirmed higher risk businesses*
- *High number of suits, liens, and judgments*

**Company:** The Kershner Co.

**Location:** West Haven, Connecticut

**Executive:** Jeffrey A. Kershner

**Problem:** Jeffrey A. Kershner pleaded guilty in October 2003 to engaging in a scheme to defraud an out-of-state lender by preparing real estate appraisals that overstated property values and contained other false information in order to obtain loans.

**The Five Cs analysis:** A query of business registrations, postal records, and public records show that the Kershner Co. was previously dissolved by forfeiture. In addition, Kershner was listed as a key executive at the Kershner Co., the Kershner-Fiorella Co., and the Templeton Mortgage Co. The search showed that the Kershner Co. and the Templeton Mortgage Co. shared the same address, while the type of business and telephone number could not be confirmed for the Kershner-Fiorella Co.

**Why is this significant?** None of these problems, taken alone, is conclusive evidence of potential fraud. But each raises a red flag, and together they present a picture of risk—due to past problems or misrepresentation—that could have been quickly recognized following a search of available records.



Decide with Confidence

---

**Continuity:** *Has the current operational status changed and is it posing new risks?*

**Continuity Red Flags**

- *Frequent management turnover or ownership changes*
- *Executive linked to multiple similar businesses, including several inactive ones in operation for a short time*
- *Different businesses share common names, telephone numbers, addresses, and executives*
- *Financial data is misrepresented or altered*
- *High payment or credit scores may reveal financial decline*

**Companies:** Ardent Research Partners, L.P.; Ardent Research Ltd; and Northshore Asset Management LLC

**Locations:** New York City, N.Y., and Chicago, Illinois

**Executive:** Francis J. Saldutti

**Problem:** The U.S. Securities and Exchange Commission in 2005 filed an emergency action to halt alleged fraudulent conduct by the two Ardent hedge funds and their parent company, Northshore Asset Management. The SEC alleged that Northshore and its principals diverted \$37 million in cash assets from the Ardent funds for personal use. As a result, the Ardent companies became illiquid and unable to meet investor requests.

**The Five Cs analysis:** In November 2003, another Ardent company, Ardent Capital, was removed from the register of companies in the United Kingdom. Shortly before that, in April 2003, Ardent Research Partners was sold to Northshore. Ardent's founder, Francis J. Saldutti, was retained as an executive with Northshore. Saldutti was a director in several companies and was linked through his business associations with Randall Goulding, who was convicted of 18 counts of fraud in 1994.

**Why is this significant?** These changes in the status of the Ardent companies—visible through routine monitoring of public and business records—represented warning signs that could have prompted regulators to examine more closely these hedge funds and their parent company, Northshore.



## Section V: Trends in Government Fraud Prevention

### Impact of Information

The continuous use of trusted, third party information sources provides a 360° view of transactional risk



The five Cs' approach can help government agencies by providing a benchmark for evaluating their own fraud prevention mechanisms. Agency leaders should ask: Where in our due-diligence processes do we apply the five Cs? Do our processes include all five, or just a portion of the five Cs? And equally important, do we have access to all available data to help evaluate entities against the five Cs? Armed with answers to these questions, agencies can develop strategies for strengthening fraud prevention.

As Dun & Bradstreet works with federal agencies to prevent fraud, our experts are seeing several emerging trends stemming from current economic downturn. Among the most significant are an increase in high-risk corporate activities associated with criminal fraud. For example, more companies are creating shell corporations to disguise business activities and are deliberately misrepresenting their business data to Dun & Bradstreet and government agencies. The hot spots for high-risk activities are California, Florida, Nevada and Texas, especially in business consulting and real estate services.

At the same time, increasing numbers of companies are displaying signs of business deterioration and financial distress that typically precede bankruptcy. For example, our business information services are reporting a rising volume of significant liens attached against companies. We also are seeing an increase in loan defaults, license revocations and the insertion of "Going Concern" clauses in audited financial statements. Since 2005, we have recorded a 40 percent increase in the annual volume of high-risk corporate behaviors, including misrepresentations and criminal charges. During that same period, the signs of business deterioration have increased 80 percent, while other information alerts associated with severe risk have increased 34 percent.

These trends have important implications for federal agencies, which are being asked to improve post-award monitoring of fraud, waste and abuse in government programs. Just because a contractor is validated as financially viable during the pre-award vetting process does not mean that it won't encounter operational difficulties during contract performance. But government anti-fraud mechanisms are not typically focused on monitoring



**Decide with Confidence**

### ***Trends in Insurance Fraud***

*Dun & Bradstreet recently participated in a California Department of Insurance (CDI) study on combating insurance fraud. Among its recommendations, the CDI advisory task force recommended that the agency acquire robust software for investigating fraud and create a centralized database containing fraud patterns, trends and other information that can be shared with participating law enforcement agencies.*

*These recommendations could also apply to federal agencies, which would benefit from enterprise-wide programs that strengthen access to business information and enable collaboration among those assigned fraud-prevention responsibilities.*

*"Reducing Insurance Fraud in California," CDI Task Force on Insurance Fraud, May 2008.*

current contractors or aimed at detecting signs of potential trouble until after the fact. As a result, agencies often fall into the trap of "pay and chase" when dealing with fraud and abuse, rather than identifying risks and resolving difficulties before they arise.

Because fraud prevention is more cost effective than fraud recovery, many government organizations are now partnering with companies that specialize in business information and due-diligence services. These companies have access to a broad range of public records and databases that can provide a multi-layered view of potential risks. In addition, business-information companies are constantly updating their databases with the most current information available and refining their due-diligence services to counter the latest criminal techniques and stay ahead of new trends in government fraud and abuse. This is important because government organizations typically don't have the resources to monitor emerging fraud practices. That's not their mission imperative. These companies also bring experience helping both public- and private sector organizations develop the processes and policies to make fraud prevention an integral part of an organization's culture and operations. Thus, a reliable partner can strengthen a government organization's organic due-diligence capabilities with comprehensive, up-to-date business information and a mission focus that delivers the latest fraud-prevention knowledge and tools.

## **Section VI: Conclusion**

Fraud prevention is indispensable to transparent, accountable government. When federal or state governments make improper and fraudulent payments, public funds are diverted from their intended purposes, such as paying needed medical bills, providing relief to disaster victims or purchasing goods and services for U.S. soldiers. White House officials have declared that they are abandoning the old model of "pay and chase," and have directed agencies to strengthen controls to prevent fraud before it happens.

The five Cs of fraud prevention provide agencies with a powerful conceptual framework for implementing this new fraud-prevention mandate. Representing "best practices" in due diligence, the five Cs approach enables agencies to benchmark their own practices and develop a blueprint for establishing stronger, more comprehensive fraud prevention controls.



**Decide with Confidence**

*For more information on D&B's  
Five Cs of Fraud Prevention  
approach, call 1.800.424.2495 or  
email [government@dnb.com](mailto:government@dnb.com)*

Will it eliminate fraud completely? No. But agencies can significantly reduce the magnitude of fraud and improper payments by using this approach and tapping into vendors whose core business is risk management and fraud prevention. Finding the right vendor partner is important, because vendors can tailor their techniques and tools to match an agency's needs. Agencies can then shift resources from recovering funds to pursuing mission-related activities. And this, ultimately, is the goal of fraud prevention: Enabling government agencies to improve performance and fulfill their public missions.