DISAPPEARING PRINTER INK P. 8 | DEVELOPING ENTIRE FRAUD PICTURE P. 24 | 5 MOST SCANDALOUS FRAUD CASES OF 2020 P. 36 | OILFIELD FRAUD P. 44 | EDITOR SAYS FAREWELL P. 50

FRAUD MAGAZINE®

A PUBLICATION OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

VOL. 36 | NO. 1 | JANUARY/FEBRUARY 2021
Fraud-Magazine.com

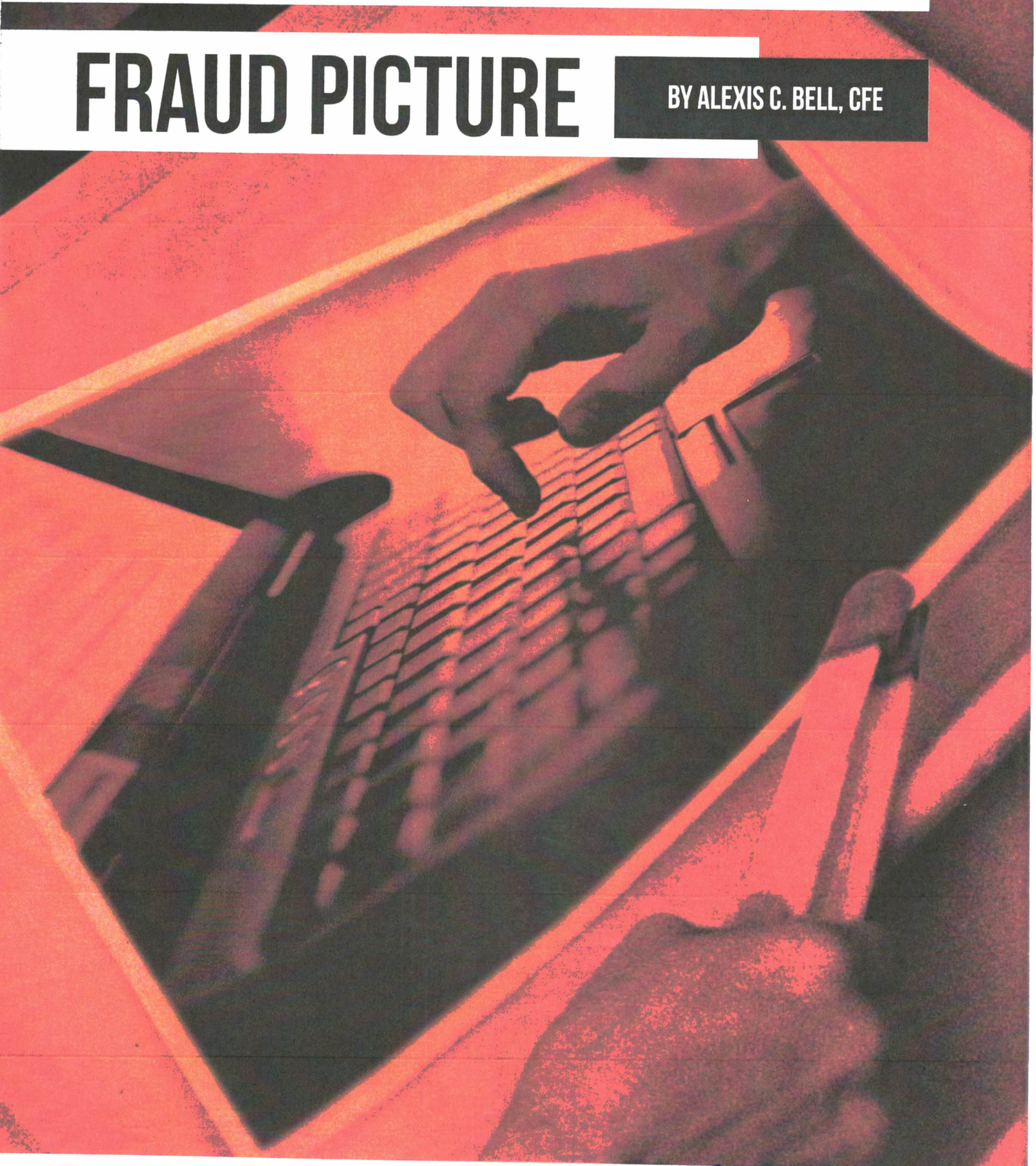
REMOTE *but* ENGAGED

Conducting investigations from afar

P. 28

DEVELOPING THE ENTIRE FRAUD PICTURE

BY ALEXIS C. BELL, CFE



Alexis C. Bell

Not every fraud scheme results in stolen money

CFEs should consider all aspects of a fraud case when calculating the impact of fraud. Here are three primary calculations when reporting the amount of fraud impact:

TOTAL EXPOSURE **FRAUD AMOUNT** **KNOWN LOSS**

Most organizations that have an internal fraud risk management program find themselves playing the loss game. They measure key performance indicators based on how much or little they lose to fraud. However, as they move up the maturity curve, sophisticated organizations understand fraud is about more than loss. To illustrate, ask yourself: Can there be a fraud committed without the presence of a loss? What about a mortgage fraud where counterfeit documents are submitted to the lender inflating their assets? What if the borrower makes all their payments on time for the life of the loan? There is no monetary loss, but the borrower received a loan they would not otherwise be entitled to based upon fraudulent documents.

Here, the *primary fraud scheme* (the main scheme) is classified as an industry specific scheme: Financial institution fraud > lending fraud > loan disbursements > loan origination > overstated assets.

The *secondary fraud scheme* (a supporting scheme perpetrated so the primary fraud scheme can be more successful) is classified as a *core fraud scheme* (those all organizations experience risk from, regardless of industry): Fraudulent statements > non-financial > internal documents.

Fraud can absolutely occur without a loss of money.

Not convinced? Let's take a look at a misuse fraud scheme: an asset misappropriation scheme under the subcategory of non-cash: asset misappropriation > non-cash > misuse. In this example, an employee with access to a bulldozer during the workweek uses it on the weekends, without permission, for the employee's separate company, which they own on the side. No cash is lost. However, there's wear and tear on that asset that wouldn't have occurred otherwise. This would be more than a mere policy violation. It would be a fraud, and remember: Fraud is a crime.

Now that you understand not all fraud produces a loss, let's examine the calculations you should report from all materialized fraud events.

REPORTING FRAUD IMPACT

In the absence of collusion, employees can only manipulate activity based on the assets, processes and records to which they have access. It is important to understand the level of risk for fraud is based on three factors: total exposure, fraud amount and known loss. Only amounts substantiated by documented evidence will be reported in each of the impact calculations. All three of these calculations are critical in effective fraud risk management.

TOTAL EXPOSURE

This is the complete exposure to a company should an employee commit fraud from the first day of their employment and with every transaction. This represents the maximum risk for fraud based on the total activity of the employee during their entire tenure. The total exposure reflects the amount of money for which their direct supervisor is accountable yet typically does not properly manage.

Many times, fraudsters are in a position of trust where a common internal control weakness is a lack of proper supervision. In the microfinance sector, for example, loans can be as small as $20 or $40. A common misconception is the notion that a loan officer distributes small amounts, and those amounts are not germane to financial statements. However, a loan officer has access to the distributions for every loan they ever made. Over the course of a long period of time, that amount can, in aggregate, become material to the organization.

Examples of total exposure calculations include:

- ***Loan officer*** — The total exposure for a loan officer is equal to the distributions for their loans during their tenure. For example, if a loan officer worked in the company for five years, calculate their distributions from the date of hire to either the termination date or the cutoff date for the analysis.

- ***Chief executive officer (CEO) or chief financial officer (CFO) —*** The total exposure for a CEO or CFO is equal to the total assets on the balance sheet. Both executives have access to all the assets under their control. Take into consideration their operating areas of responsibility. If they are at the international level, use the consolidated balance sheet at the global level. If the executive is at the subsidiary level, use the balance sheet for their operating company.

Use the most current date relative to the time frame in question. For example, if it is now February and there are known fraud amounts committed in October of last year, and the fraudster was still in the company as of the first week of December, the balance sheet total assets figure should be as of the end of November.

FRAUD AMOUNT

This is the total amount of fraudulent transactions. Keep in mind that this is the sum of the absolute value of the transactions. For example: (one transaction for $12,345) + (one reversal of $6,789) = (fraud amount of $19,134).

Getting this number wrong could significantly understate the fraud amount. In this example, one transaction for $12,345 and one reversal of $6,789 calculates as a fraud amount of $19,134 because the mathematical equation would be: |$12,345| + |-$6,789| = $19,134.

The amount of the fraudulent transactions is meaningful in classifying criminal charges. In some countries, the classification can be the difference between misdemeanors and felonies where there's a monetary element to the classification. The classification can also affect the determination between the amount of mandated prison terms (jail time), and the calculation of fines and penalties.

The amount of the fraudulent transactions is meaningful in classifying criminal charges. In some countries, the classification can be the difference between misdemeanors and felonies where there's a monetary element to the classification.

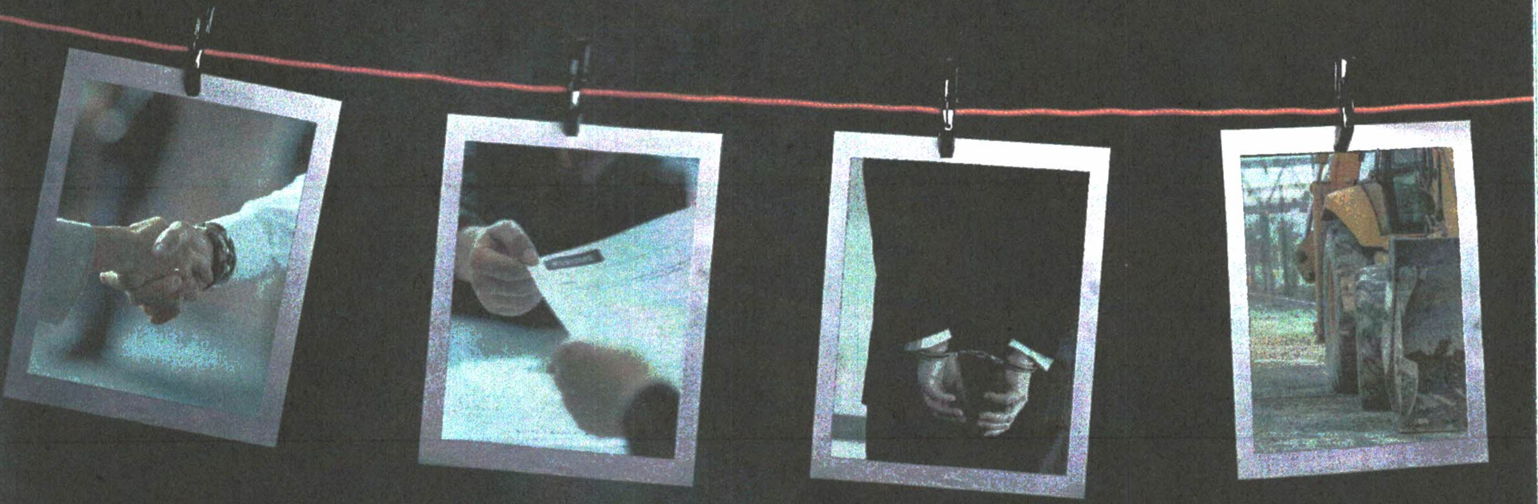
To better understand this concept, ask the question, if someone entered a fraudulent transaction into the system for $500 and then fraudulently reversed that entry, did fraud occur? Because the person entered the transactions fraudulently, the answer is yes. In this example, the fraud amount is $1,000.

In cases of financial statement fraud involving revenue recognition, one benefit to the fraudster lies in the shifting of the timing of the transactions. The **core fraud scheme** is classified as: *Fraudulent statements > financial > revenue recognition > timing differences (overstatements)*.

Recognizing revenue before it is earned in one month and then reversing it the next month is still fraud. This is a common scheme in shifting revenue from January to the previous month of December to meet analyst projections at year end. This type of fraud affects management bonuses and can manipulate the stock price for publicly traded companies.

Another example is: (one transaction for $2,468) + (one transaction for $-3,690) = (fraud amount of $6,158)
Where: |$2,468| + |$-3,690| = $6,158.

Fraud can occur without a readily identifiable amount. In cases of a counterfeit document such as a fake resume (classified as a core fraud scheme: fraudulent statements > non-financial > employment credentials), it is difficult to assign a number based on transactions. Therefore, you must calculate the total salary and benefits (typically around 30 percent of salary) given to the employee as the fraud amount. This is income, associated benefits and any sales commissions, *"Fraud can absolutely occur without a loss of money."*



if applicable, they would not have received without the fraud act.

KNOWN LOSS

This is the known amount of fraud based on evidence gathered during the course of the investigation. Remember, only amounts substantiated by documented evidence will be reported in this impact calculation. Known loss will often be presented as net of recovery (when you identify and recover over payments and under-deductions to suppliers) or restitution (recompense for injury or loss: restoration of something stolen and returned to its owner).

It is important to understand the known loss amount for filing insurance claims to mitigate the impact of the loss (when available) as well as to submit during criminal proceedings to seek restitution from the fraudster and for civil damages in a lawsuit.

Total restitution includes at a minimum the cost of the investigation, the cost of litigation and the amount of loss. In some cases, it can also include other factors to make the company whole from the fraud act(s), such as the cost of monitoring imposed against the company from a deferred prosecution agreement. Thus, the known loss is just one part of the total restitution calculation.

Another consideration of known loss is that it is the amount known at that time. It is important to understand that the investigation might not uncover all aspects of the total fraudulent activity. Investigations are limited by the amount of resources they have — time, people, tools. Some schemes might remain hidden. Therefore, the verbiage includes the word "known" because that is the amount that is supported by evidence as of that point in the investigation.

UNDERSTAND THE FULL IMPACT OF FRAUD BEFORE FINALIZING YOUR REPORT

Consider three primary calculations when you are reporting the amount of fraud impact: total exposure, fraud amount and known loss. They are distinct from each other. Each conveys meaningful information that an organization should communicate to stakeholders.

There is value in the ability to report these figures to management. It gives them the information they need to make informed decisions about fraud risk and how they can allocate resources to effectively manage that risk. Likewise, the board can make informed decisions about how best to fund and support the fraud risk management program. ▪ FM

Regent Emeritus Alexis C. Bell, CFE, is the founder and managing partner of Fraud Doctor LLC. Contact her at alexis.bell@fraud-doctor.com.