REVISITING BENFORD'S LAW WITH ADDED AI HORSEPOWER

For over a decade, CFEs, auditors and analysts have used Benford's Law to identify journal entry irregularities. Today, this analysis method remains relevant as ever as new applications using AI and simulation could bring Benford's Law to the forefront of your fraud risk management controls.

If you've passed the CFE Exam or the CPA exam, you're familiar with Benford's Law. This principle observes the unexpected regularity that in any large, randomly produced set of natural numbers, such as streamflow statistics, town and city populations, or corporate sales or payment amounts, around 30% of the numbers will begin with the digit 1, 18% with 2, and so on; with the smallest percentage beginning with the digit 9. Accountant and fraud investigator Mark Nigrini, Ph.D., popularized it in his book "Digital Analysis Using Benford's Law," first published in 2001. You've probably used Benford's Law to analyze accounts payable amounts, purchasing card data and journal entries in your search for irregularities or risk areas. By searching for cases where the expected proportion of the first (as well as the first two, or even first three) digits in a payment or transaction stream don't conform, you'll find indications that someone might be overriding a control or manipulating the numbers — disrupting the digit patterns.

For this Innovation Update column, I'm going to describe how to take Benford's Law to another level using artificial intelligence (AI) and automation so that fraud examiners may use Benford Subset Divergence Analysis (BSDA). Using BSDA, we can identify subsets such as business units, expense categories, vendor categories and any other type of filtering criteria generating the most significant nonconformity under Benford's Law instead of looking at an entire dataset one time-consuming filter at a time. I was fortunate enough to collaborate with Nigrini to explore this concept further and test a few scenarios under his supervision.

A dash of theory

A Scientific American article published last year tells the story of how Benford's Law was originally identified in 1881 by astronomer Simon Newcomb. (See "What Is Benford's Law? Why This Unexpected Pattern of Numbers Is Everywhere," by Jack Murtagh, Scientific American, May 8, 2023, tinyurl.com/y7mne8jb.) Physicist Frank Benford made the same observation in 1938 and popularized the law — and attached his name to it. Some references attribute both names to the model, referring to it as the "Newcomb-Benford Law." You may also see it referred to as the "law of anomalous numbers." In many real-life sets of naturally occurring numbers, the first digit is likely to be small, starting with a 1, 2 or 3, for example. In sets that obey the law, the digit 1 appears as the first digit about 30% of the time, while 9 appears as the first digit less than 5% of the time. The first digit probabilities for 1 through 9 are as follows (zero isn't admissible as a first digit even though we need to have the zero in some cases, such as 0.07):

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
CEO OF KONA AI

d	*P* (*d*)	Relative size of *P*(*d*)
1	30.1%	
2	17.6%	
3	12.5%	
4	9.7%	
5	7.9%	
6	6.7%	
7	5.8%	
8	5.1%	
9	4.6%	

Figure 1: Benford's first-digit probabilities

The most effective Benford-related test for financial data is the first-two digits test because it results in smaller samples of notable items. This test works especially well in identifying large groups of transactions just below internal control thresholds or perceived thresholds, such as when a company's vendor policy stipulates that any invoice over $5,000 requires a second approver or additional documentation for payment. The incentive for fraudsters is to keep an invoice just under that amount, perhaps maxing invoices out at $4,900 or even $4,999 to stay under the threshold. In Figure 2, you'll see a spike in invoices starting with the digits "49" and "48." Those digit combinations should be occurring around 0.89% of the time, but in fact, the digits occurred around 1.1% of the time (hence the spike). This is an indicator of someone artificially keeping invoices just under the $5,000 threshold.

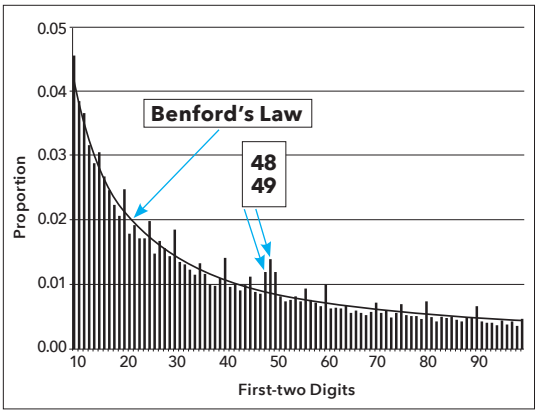


Figure 2: Two-digit example

In my interview with Nigrini, he pointed out that Benford's Law can be used to help fraud examiners or auditors identify:

- Large counts of fictitious journal entries that are below auditor-testing thresholds or corporate policies.
- Ridges and valleys in data — ranges in a graph where data clusters over or under the Benford's Law line can be signs that large numbers or fictitious entries have been created.

- Irregularities in the general ledger, such as unusually high duplications of the same dollar transactions. These irregularities may or may not be fraud, but could be erroneous.

The challenge with the current approach

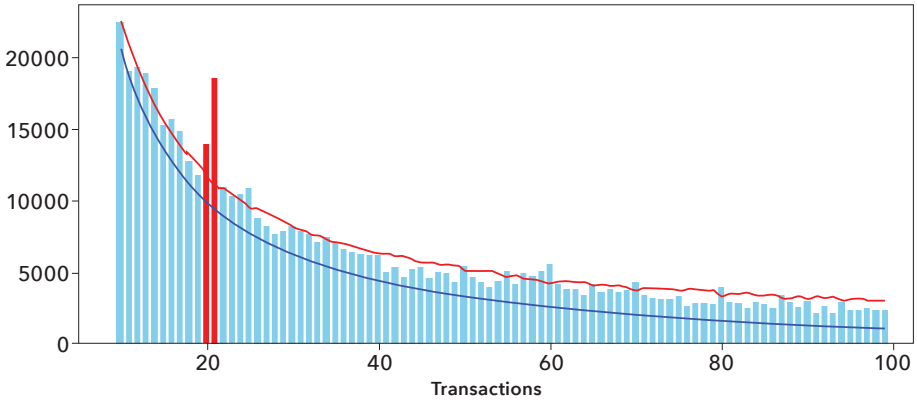
As simple and powerful as Benford's Law is to run on datasets, it does have a limitation, which stems from looking at large datasets in an aggregate, linear fashion. Nigrini recommends that fraud examiners look at datasets of no less than 2,500 but ideally greater than 5,000 transactions when using the first-two digits test. In large global companies, the 5,000 threshold is easy to obtain as journal entries can span hundreds of thousands, if not millions, of transactions. The challenge lies with the ability to spot rogue behavior within a small business unit, or a group of individuals within a geographic area or other classification when looking at transactions in the aggregate. Risk transactions not matching Benford's Law can be easily "washed out" given the sheer volume of today's transactional activity.

Data visualization tools like Tableau or PowerBI can be helpful to filter down large bodies of data on a case-by-case basis, using geography, expense type or other criteria. The goal is to home in on potential rogue activities within a subset of the aggregate data in a way that targets and detects anomalies across thresholds. However, this approach can still be time-consuming given the hundreds, if not thousands, of possible filtering combinations between geographies, business units, expense types, payment types and other factors used to drill into data.

But what if we could get a machine to run all these scenarios, instead of manually filtering one at a time?

The AI booster

In speaking to Nigrini about the challenge of running multiple filtering scenarios manually to find anomalies, we brainstormed ideas on how to automate this scenario process to identify only the subsets that drove the highest Benford's Law deviations. Working with Kona AI's head of data science, Roopak K. Prajapat, we analyzed a vast dataset spanning several hundred thousand invoice payments totaling more than $3 billion in spend. The aggregate data seemed to follow Benford's Law rather nicely with a few immediately noticeable deviations, such as in payments starting with the digits 20 and 21.



We then used BSDA and automation with elements of robotic process automation (RPA) to run the data across five distinct classifications to identify the subsets with the largest deviations from Benford's Law, subject to the 5,000 minimum sample size constraint. The variables we ran during our testing included:

- Vendor category.
- Payment type/method.
- Country.
- General ledger (GL) account.
- Document type.

The model ran more than 17,808 combinations in about 21 minutes of data processing on commodity hardware to identify the subsets with the largest divergence. (Compare that to the time it would take to do it manually.)

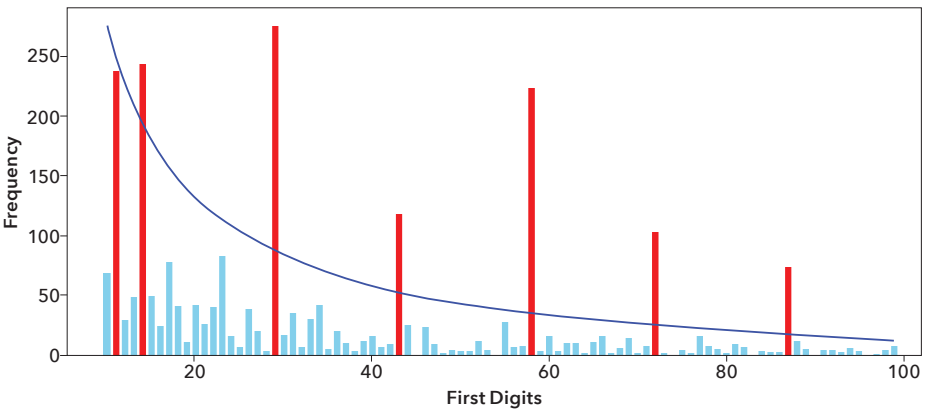
The most anomalous subset turned out to be a certain vendor — we won't name them here — with the attributes listed in the table on the right.

We then fed those transactions to a predictive, machine-learning model to find "more-like-this" statistically similar transactions to further enhance the results. The revised Benford's analysis lit up with all sorts of anomalies within this subset.

Vendor Number	0000CCUS10
Payment Method	N-US SUB USD NETTING
Remit Country	US
GL Account:	<null>
Document Type	CS-CO Posting Secondary

Key observations

- **Anomalies:** The large red spikes, especially around digits like 11, 14, 29, 43, 58, 72, 87, etc., in the graph below suggest that certain transactions are occurring much more frequently than



Benford's Law predicts. This is a red flag for anomalies or irregularities.

- **Potential risks:** Deviations from the expected distribution could point to data manipulation, fraud or specific transaction patterns that warrant further investigation. The nature of the spikes might suggest either manual adjustments or systematic biases in the transactions recorded under this GL account.
- **Compliance concern:** Given that Benford's Law is often used in fraud detection, the significant deviations in this analysis could signal that the transactions under the "N-US SUB USD NETTING" GL account require closer scrutiny. This may involve investigating why certain transactions or groups appear so frequently compared to others.
- **Equally distant anomalies:** A stark visual pattern highlights that the anomalies occur about equal distance from one another. It's worth identifying the underlying reasons to uncover further insights.

We provided those transactions to our customer for investigation, who deemed them anomalous enough to launch an investigation, which is ongoing. The investigators of this case shouldn't only review vendor CCUS10 but also the related subsets, such as transactions in 2023 and 2022, or expenses posted to the same expense or asset account.

Benford's Law for the future

Benford's Law has been, and always will be, a useful fraud detection tool. Now, with the use of better technologies and automation, techniques like BSDA allow investigators to identify the most anomalous subsets quickly and efficiently, turning what was once a time-consuming process (seldom even attempted) into a powerful automated tool for uncovering hidden fraud patterns in big data. ■ **FM**

Vincent M. Walden, CFE, CPA, is the CEO of Kona AI, whose company mission is to empower compliance, audit, and investigative professionals with research-driven, innovative, and effective analytics to measurably reduce global fraud, corruption and enterprise risk. He works closely with CFEs, internal auditors, compliance, audit, legal, and finance professionals and welcomes your feedback and ideas. Contact Walden at vwalden@konaai.com.