A global “quick-service” (i.e., minimal table service) restaurant business with thousands of locations accelerated its employee theft-and-error detection rate at the cash register by approximately threefold. Enhancements included the risk analysis of geographic regions, stores, employees and point-of-sale (POS) transactions plus integrating “machine learning” for improved fraud detection.

The company’s team of analysts embarked on this journey by developing multiple fraud scenarios that modeled the known behavior of employees stealing from the company’s cash registers. The models calculated fraud schemes by combining multiple data sources, which included POS, store location information and employee scheduling. Then, the machine-learning models used statistical benchmarking and dozens of algorithms to score and rank risks that potentially existed in transactions, employees, stores and regions.

The team displayed the results in data visualizations that provided a global view of risk specifically tailored to the organization’s operating and reporting needs. As the team discovered and confirmed fraud schemes, it added those specific fraudulent transactions into the model to improve the results of the system.

Machines that learn
This case study shows the advantages for retail and restaurant organizations that incorporate machine learning and visual techniques into their loss prevention and anti-fraud controls, rather than just relying on traditional exception-based reporting (EBR) systems. Machine learning “is an application of artificial intelligence that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.” (See “What is Machine Learning? A definition,” Expert System, tinyurl.com/y9l3sul7.) A well-known example of machine learning is IBM’s Watson.

Because of the reliability of the findings and transparency of the reporting, it’s possible to make the analytics results more actionable and do such things as implementing targeted fraud awareness campaigns or proactively deterring fraud by implementing additional controls at cash registers (the POS). This reliability increases when we analyze more data via machine learning with the model continually improving accuracy over time.

“While most companies have established internal controls that address ‘shrinkage,’ they generally lack recent analytics and technology innovations, specifically machine learning, and could be leaving money on the table,” says Michael Gottlieb, EY’s global leader of restaurant services.

Measuring the cost of fraud and administrative errors at the POS
Shrinkage is defined as the loss of inventory attributed to factors such as employee theft, shoplifting, administrative error and vendor fraud that benefits the customer, according to the National Retail Federation. The National Retail Federation’s 2017 National Retail Security Survey reported the average shrink rate of 1.44 percent as a percentage of U.S. retail sales, which cost the overall U.S. retail economy $48.9 billion in 2016. (See tinyurl.com/ygoswtr15.)

According to the survey, employee internal theft accounted for 30 percent of that 1.44 percent shrinkage figure. When combined with internal administrative and paperwork error (21.3 percent), this accounts for more than 51
percent of total retail shrink (or 0.734 percent of retail sales). For a retailer with $1 billion in sales, 0.734 percent translates to $7,340,000 in lost profits per year. It’s time to get some of that money back!

We begin with the premise that companies should design their fraud detection analytics programs with the goal of improving fraud prevention and detection, as well as internal administrative error, by distilling numerous or complex data sets so anti-fraud professionals can make substantive decisions and act on them.

Analytics can help retail stores and restaurants by defining companies’ loss-and-waste profiles and identifying specific risk areas. An effective analytics program framework will enable risk detection and seek to measure the total dollars responsive to potential fraud risk areas, which in turn helps management respond, remediate and potentially implement improved controls to increase fraud prevention. (See Figure 1 on page 18.)

However, traditional anti-fraud, POS and internal-controls programs can sometimes underperform — or fail to detect fraud and administrative errors altogether — by gathering false or ambiguous information for estimating the extent and types of potential loss and shrink. In our experience, adequate controls typically aren’t integrated into a loss-prevention methodology or suite of tools with the goal of reasonably calculating accurate projections of loss and learning from past fraudulent events.

Most retailers try to detect fraud with outdated EBR techniques that identify simple rules-based transactional anomalies in dollar amounts, percentages and frequencies for employees and stores. These rules might include simple matching, sorting, filtering or arithmetic procedures that require anti-fraud professionals to ask questions of the data based on what they currently know. This approach often results in too many false positives and/or false negatives to be comprehensive or effective, and to justify a reasonable return on investment (ROI).

Anti-fraud professionals who are focused on loss prevention can be at risk of spending too much time and devoting too many resources while chasing down false leads. This can happen when their analytical systems give them too many “false positives” (i.e., transactions that meet certain risk indicators but indeed aren’t erroneous or fraudulent) or “false negatives” (i.e., when erroneous or fraudulent transactions are underreported and missed by controls).

The primary purpose behind rules-based algorithms, or any anti-fraud loss prevention program, is to infer human behavior from the data of known POS scams, such as when a cashier rings up an order, receives payment, delivers the order, cancels the order and then pockets the money after the customer walks away.

Machine learning goes beyond EBR at the POS and lets the data define itself

CFOs, finance, internal audit and anti-fraud professionals can benefit by enhancing their EBR-based loss prevention systems with machine learning. The prize? Significant financial recoveries and fraud prevention. “At Bloomin’ Brands, Inc., we are constantly looking at ways to reduce shrinkage in the restaurants, including the use of statistical and machine-learning techniques to reduce false positives and increase our detection rates,” says Derek Kolano, vice president of internal audit at Bloomin’ Brands Inc., which owns and operates several restaurant chains, including Outback Steakhouse, Fleming’s Prime Steakhouse & Wine Bar, Carrabba’s Italian Grill and Bonefish Grill.

“Companies that use the right combination and proportion of rules-based, sequential, statistical and predictive machine-learning models mitigate the shortcomings of simple EBR systems and decrease false positives and false negatives,” says Eric Johnson, EY executive director and data scientist.

“Sequential models act as a timeline, which enables loss-prevention teams to see trends over time. Statistical models act as regulators and stabilize systems to enable ‘like-to-like’ comparisons so that explainable statistical anomalies don’t unduly influence the final results. Machine learning builds on these successes by improving the models based on past anomalies or events,” says Johnson, who’s developing these advanced loss prevention technologies.

“Rules-based, EBR loss-prevention platforms are like streetlamps at night on a long street. The light may not cover the entire length of the sidewalk, and you may still walk in the darkness,” he says. “Machine-learning algorithms, however, serve as your night-vision goggles by shining light on new patterns of fraudulent behavior as employees adapt to new controls or conduct fraud schemes in different ways.”

Fraudsters can scheme in a variety of ways at the cash register. Behavioral analytics combined with machine learning can enhance your POS fraud-detection program by uncovering these schemes through scoring the highest-risk geographies, stores, employees and transactions. (See Figure 2 on page 18.)
Common POS schemes
Here are just a few of the common fraudulent cashiers’ retail and restaurant schemes where all of the techniques described in this column played a role in detection.

Canceled transactions: Rings up an order, receives payment, delivers the order and then cancels the transaction before pocketing the amount received. It’s simple, but often difficult to spot.

Preferred discounts: Selling items to family and friends at employee discount prices. They can take the scheme one step further by returning items for full-price refunds at different locations without receipts.

Sweetheating: Giving free merchandise or discounts to family and friends without proper authorization, often by simply not scanning products. This category also can include false returns.

Refunds: Ringing up false refunds and pocketing the amounts, which could cause an illusory inventory shortage. As part of this scheme, an employee might prepare a refund voucher with an assumed name and address.

False returns: Here are a few of the numerous schemes in this category:
- Wardrobing/renting: Purchasing merchandise with the intent to return the item the next day — for example, a dress for a big date or a big-screen television for the Super Bowl.
- Returning stolen merchandise: Shoplifting and then returning items for purported refunds.
- Receipt fraud: Using reused, stolen or falsified receipts to return merchandise for refund.
- Underringing: Ringing an item at less than its listed price, collecting the full value of the item and pocketing the difference.

Training fraud: Managers often have the authority to program cash registers so sales aren’t recorded when they’re training new employees. Employees abuse this function when they purchase store goods during training modes and don’t document the transactions.

Questions for your CFOs and anti-fraud professionals
When you evaluate your loss-prevention program, consider these questions for management:
- Can you measure your annual shrinkage from fraud, waste and abuse?
What fraud-detection tests and controls are you deploying? Are they all exceptions-based results?

What’s your current spending on loss prevention (including technology and human cost) along with the associated ROI?

How’s your organization using machine learning? Can your organization apply it to fraud prevention and detection?  

Vincent M. Walden, CFE, CPA, is a partner with EY. Reach him at: Vincent.Walden@ey.com.

These EY team members contributed to this column: Eric A. Johnson, Mohan Kundur, Jay Sonbolian, Michael Gottlieb and Arpit Bothra.

Check your back
Collusion is one method by which bad actors can circumvent effective internal controls. It also makes fraud detection extremely difficult, if not impossible, unless you have inside information — such as a tip — to help uncover it. Also, complicated accounting systems, fragmented sales structures and language differences raise the difficulty of conducting internal fraud investigations.

Finally, C-suite fraudsters can easily erect roadblocks or even sabotage your fraud examination. Therefore, we should make sure that we have the required independence and support from those charged with the governance of the organization before tackling a fraud examination.  

Steve C. Morang, CFE, CCEP, CIA, CRMA, is a senior manager at a Northern California-based CPA firm and president of the ACFE’s San Francisco Chapter. His email address is: steve.morang@yahoo.com.

BIG FRAUDS, CONTINUED FROM PAGE 9

Identity theft is a common type of fraud that does not discriminate. Anyone can be targeted; the victim might be a college student, a retiree, a schoolteacher or a successful attorney. Even businesses can be victims of identity theft.

This course discusses the types of identity fraud and provides guidance to help prevent you and your community from becoming victims of identity theft.

Key Takeaways:

- Methods used by thieves to steal personal and business information including social engineering, pretexting and hacking
- Types of identity theft schemes including financial, insurance, medical and business
- Tips for preventing identity theft for individuals and businesses
- Actions to take if you have become a victim of identity theft
- Tips for educating employees to protect your organization from identity theft

Visit ACFE.com/IdentityTheft to learn more.