COMPLIANCE WEEK

{RISK MANAGEMENT}

Tips for detecting pandemic fraud risks at your company

With the pandemic tide out, here are some related frauds likely already occurring that corporations should be watching for.

BY AARON NICODEMUS, COMPLIANCE WEEK

"Only when the tide goes out do you discover who's been swimming naked." – Warren Buffett

The coronavirus pandemic is placing unbelievable strain on all facets of the world economy, with stay-at-home and shutdown orders shuttering some industries and disrupting most others. The abrupt shift to working from home has created new and varied opportunities for fraudsters and criminals to ply their trades.

But there are also opportunities to identify illicit behavior that started before the pandemic hit, and compliance practitioners have a crucial role to play in identifying and ferreting out new fraud schemes while also exposing previously undetected activity.

"If someone has been diverting funds, now is the time to find them," said Daniel Wager, vice president of global financial crime & compliance with LexisNexis Risk Solutions.

One thing employers should remember is activity that was considered normal before the pandemic is not normal now, compliance professionals say. Monitoring of employee activity and financial transactions since March must be viewed through this new lens. Vendor payments that continue unabated to pay for nonessential goods and services—despite deep corporate cost cutting or a spending freeze—deserve a hard look.

Salespeople who continue to submit expense reports similar in size to their pre-pandemic spending should raise eyebrows because they likely aren't traveling at the moment, says Andy Miller, chief analytics officer at compliance software company Lextegrity.

"So many companies are not continuously monitoring their spending right now. It's hard to do this detective work in normal times, and it's even harder to do in a pandemic," Miller said.

Traditional compliance controls have been weakened by work-from-home scenarios, because it is harder to monitor all potential means of communication, like second personal cell phones, social media, and chat apps like WhatsApp and Weibo.

"People aren't working in that physically monitored environment, and so it's harder to track who they're talking to and what they're saying," said Lee Garf, general manager of NICE Actimize, a financial crime and compliance vendor. "There are also new trading patterns emerging, so you have to fine-tune your alerts quickly and easily to respond to them."

Here are some pandemic-related frauds that are likely already occurring that financial institutions and corporations should be watching for, as well as pre-pandemic frauds that could be exposed, with advice on how to spot and report them.

Fraud in the 'barnacles'

Tesla Chief Executive Elon Musk said in a 2018 conference call that his company would start "scrubbing the barnacles off" with what was described as a new, brutal regime with regards to contractors, according to a story in the Mercury News of San Jose, Calif.

Corporate cost cutting and frozen budgets should be viewed as an opportunity to examine expenditures with vendors and contractors, said Miller.

"Some employees may have an emotional attachment to a vendor, and that might provide the pressure and rationalization to keep that spending going," he said.

If a company has cut spending, non-critical spend-

ing should be slashed across the board. Look closely at non-critical line items whose funding isn't affected, he said.

Another way fraudulent transactions might appear is through a change in middle management. Say three managers regularly review vendor spending or monthly reimbursements, but due to changes in staffing or priorities, those responsibilities are reassigned. The new set of eyes might lead to hard questions being asked on specific spending items.

Pre-pandemic fraud schemes may come to light during the pandemic, as changes in patterns and behaviors uncover bad behavior. Fictitious vendors could be exposed when one person who had been approving them is laid off or reassigned, Miller said.

One way to red flag expenditures for fraud is to set up alerts that look for similarities between employee addresses, phone numbers, and tax identification numbers with those listed for the potentially fraudulent vendor. Pore over non-critical expenditures, and keep going past the biggest ones.

"You have the opportunity to look up and down the ledger and ask, 'Why are we spending money on this?'" Miller said. "People mostly do the right thing, but you have to be vigilant."

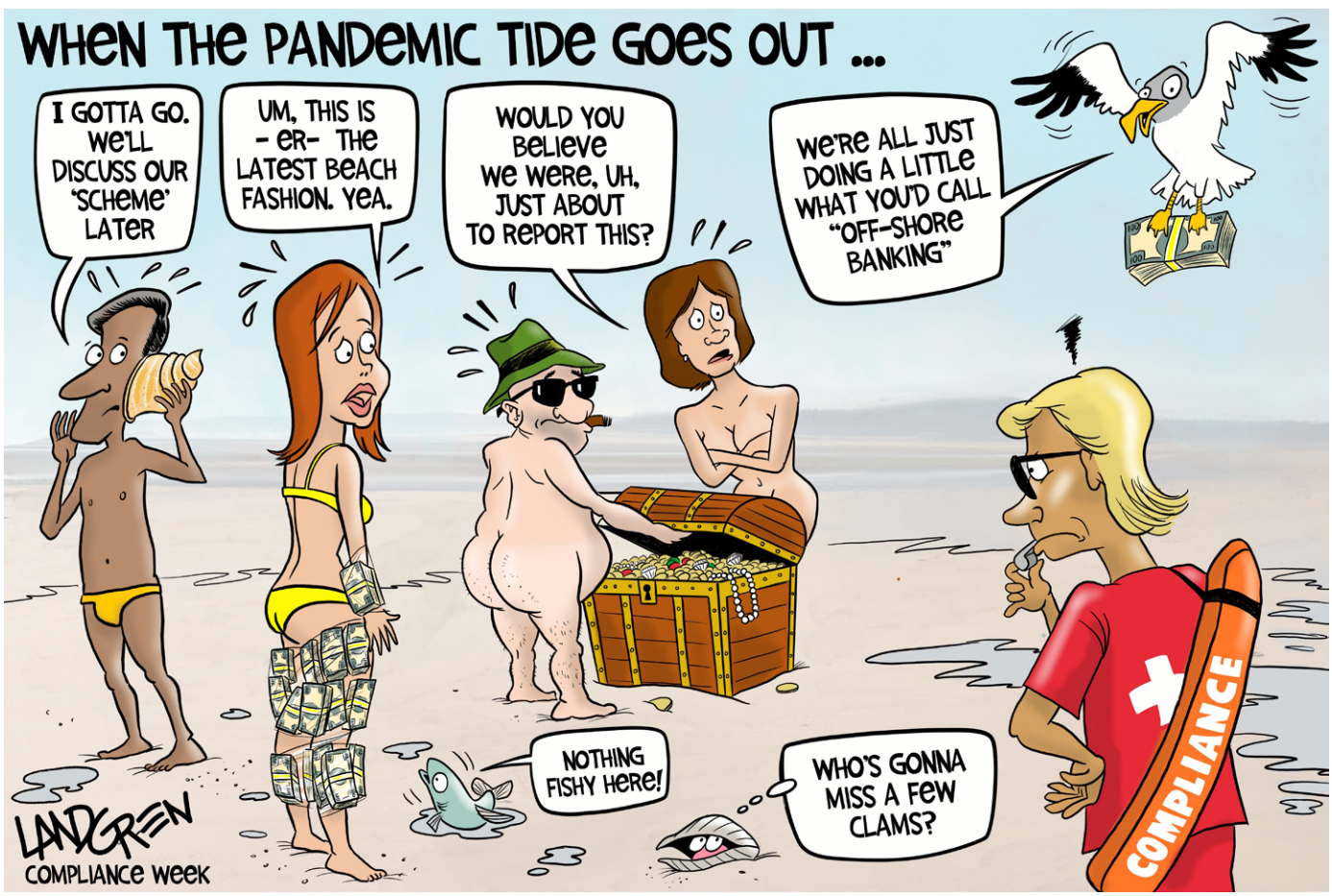
The fraud tends to be buried in the barnacles; the small expenditures, not the whale.

Pandemic financial crime red flags

Monitoring employees who are working from home is harder than ever, says Garf. This is especially true of traders and brokers who could take advantage of the weaker oversight to pursue any manner of stock and insider trading schemes.

Typical trader activity involves a call; then a trade transaction; then a follow-up email, call, or text. In a traditional setting, that traders' access to non-approved lines of communication is severely limited. But working from home has upended those protocols, Garf said.

No initial call could be an indication that the working-



from-home trader is using non-compliant, non-approved communication tools to discuss a murky deal.

"You also want to look at what a trader has done in the past, and also what he's doing compared to his peer group," Garf said. "You want to ask yourself, 'Does this person stand out?'"

There are also more opportunities for market manipulation, where a trader coordinates with another trader to manipulate a stock's value, then short sell it. A lack of transparent communication around the transaction could be a red flag, Garf said.

"The system can't always predict the creative ways that people will cause problems," he said. Once an organization uncover new types of bad behavior, they can adjust their compliance software to search for those new patterns, he said.

Will illicit cash prove tempting to small businesses?

Traditional means to launder illicit cash have been significantly disrupted, said Wager, a former agent with the U.S. Department of Homeland Security and U.S. Customs Service. With the economy effectively shut down, there are fewer avenues to co-mingle illegitimate cash with money moving through the legitimate economy, he said.

"The best positioned individual in this current environment to make money are the illicit financiers," he said.

But the government may have thrown criminal enterprises a money laundering lifeline—the Paycheck Protection Program (PPP), Wager said. More than $510 billion in PPP loans have been distributed to small businesses through May 30, to help keep them afloat while their businesses are shut down, according to CNBC. Businesses can turn the loans into grants if they can show they used 75 percent of the money to fund their payroll.

Wager says the PPP loans are ripe for abuse. The Georgia reality star who received a $2 million loan for a trucking company that did not exist or the New England businessmen who received over $500,000 to fund payroll for defunct companies are just the tip of the PPP fraud iceberg, he said.

Illicit financiers could approach legitimate small businesses with an offer to launder cash. Here's how it would work: The financier offers to give the legitimate but struggling business owner cash to cover his payroll. The business owner then writes checks to the financier's associates, real or imagined. The business owner keeps a cut, and the financier has successfully laundered the money.

The transactions may not create red flags for the financial institution processing these transactions because the PPP is a legitimate source of income.

Another avenue for money laundering is real estate. Imagine the small landlord who accepts cash monthly for rent payments. About a quarter of renters in New York City did not pay rent in May, according to a survey by The Real Deal, a New York real estate publication.

An illicit financier could take advantage by offering to prop up the flagging rents. The landlord cuts checks to the financier's friends and associates for ghost repair work, and voila, the cash is laundered. The financial institution may not notice because the total rent payments for May match what the landlord deposited earlier in the year.

> "So many companies are not continuously monitoring their spending right now. It's hard to do this detective work in normal times, and it's even harder to do in a pandemic."
>
> Andy Miller, Chief Analytics Officer, Lextegrity

"The PPP is a perfect storm of pressures and opportunities for the desperate business owner to accept drug cash," Wager said.

What's a financial institution to do? Start by appointing a special custodian to begin reviewing these PPP loans for signs of fraud, Wager said. Re-examine transactions by companies receiving PPP loans. Figure out what should be happening to the revenue streams, and if it doesn't match reality, create alerts that search for new anomalies. React more quickly if a business owner stops responding to the bank's inquiries.

Other anomalies to look for include long-shuttered businesses appearing to be in operation, false claims to ownership, lack of licensure or registration, and prior histories of fraud or other criminal behavior, Wager said.

Once fraud is discovered, do not hesitate to report it to government.

"The best entity to recover your funds, in many cases, may be the government," he said. "The government is brilliant at seizing funds." Filing a civil suit through the court system looks to be a long and frustrating process for the foreseeable future. ■