Issue #33
January 2016

GREAT AMERICAN and LOWERS & ASSOCIATES

Fidelity / Crime Observer

A Temporary Problem

While it is true that some employers staff their companies entirely with temporary employees, most are hired seasonally by retail and related businesses, including transportation and manufacturing. These "temps" may have no loyalty to their temporary employer, and may even regard their new jobs as an opportunity to walk off with inventory, cash, or the personal information of customers. Even if the amounts taken are small, the totals in inventory or cash receipts shortage can mount up over a few weeks.

An example of this type of loss is demonstrated by temps processing a popular, widely advertised product. They would toss boxes of this product into a dumpster when they were momentarily unsupervised, and they or their accomplices would retrieve the boxes at a later point. They then sold the items at a large discount, which in addition to the fraud loss, drove down the retail price considerably. By the time the company's inventory procedures discovered the loss, the damage was done, and the temps couldn't be found.

Another temp working in a firearms manufacturing plant was directed to take a small number of defective rifle barrels to a scrap dealer, and return with a check for the salvage. He then realized he could do this repeatedly, and marked good barrels as being defective. After repeated salvage transactions, the manufacturer's shelves of imported barrels were almost empty; he could not fill orders; and the temp profited greatly.

In yet another case, a high end retailer's bookkeeper noticed that a certain cash register had an unusually high number of refunds. Whenever the temp manning this register received a large payment in cash, he made a note of it, and later in the day processed a cash refund. In the Christmas rush, this wasn't noticed until the end of the month, when the temp was long gone. At the same time, the employer received the results of a belated criminal records check showing that the temp had a history of stealing from employers and forging checks.

So how does an employer prevent this type of fraud? First, whether using a temp agency or directly hiring temps, the same background check procedure should be followed. The employer should also verify that the agency's employee dishonesty insurance covers the loss of customer property. Either the agency or the employer should have a copy of the employment application, a copy of a government issued photo id or driver's license, and contact information for dependents or relatives. There should also be a contract between the agency and the employer detailing the agency's loss responsibilities.

Second, security procedures should be in place, including continual video surveillance, with daily monitoring of the security tapes, as well as close personal supervision. Odd or aberrant behavior should be noted. Shipments and deliveries should be tracked closely. Sales variances, cash register errors, and cash shortages should be monitored daily. In warehousing or manufacturing operations, outgoing trucks should be inspected by security personnel or dispatchers to ensure the trucks' contents match the shipping documentation. If a running inventory system is utilized, a quick visual inspection should be made at the end of each day, or the next morning, to ensure that inventory on hand matches the books.

Finally, temps should be closely supervised throughout their employment. Too often, once the temp is trained, they are monitored the same as regular, long term employees, giving them more of an opportunity to steal.

If a loss is discovered, the police, the temp agency, and the company's employee dishonesty carrier should be notified immediately. Most employee dishonesty policies cover theft by temporary employees, however the agency's policy should be primary. Employee dishonesty costs U. S. businesses millions per year. Do not be a victim!

By William F. Marston, Vice President, Crime Claims
Great American Insurance Group
Fidelity / Crime Division

Contact List

Great American Insurance Group

Dennis Burns, SVP
Fidelity / Crime Division
212.513.4017
dburns@GAIC.com

Lowers Risk Group

Steve Yesko, ARM
Director, Business Development
540.338.7151
syesko@lowersriskgroup.com

Inside This Issue

Not If But When: How to Avoid Becoming the Next Target of FinCEN AML Enforcement

If you run a business that facilitates or conducts money transactions, or transactions in other liquid commodities, you are no doubt aware of FinCEN. Rest assured that FinCEN is aware of you, too. And we predict it's only a short matter of time before their foreshadowing of AML enforcement actions against the cash servicing and transport industry becomes a harsh reality.

The Financial Crimes Enforcement Network (FinCEN) is the arm of the U.S. Treasury charged with investigation and enforcement of Bank Secrecy Act provisions intended to block the financial sources of illegal and terrorist organizations. Traditionally, the BSA applied to common financial institutions like banks and credit unions. But as banks began to offload services to third party vendors and the number of money-related businesses like check cashers and wire transfers proliferated, the BSA has been applied to an ever-wider array of businesses.

FinCEN is the arm of the US Treasury charged with investigation and enforcement of Bank Secrecy Act provisions intended to block the financial sources of illegal and terrorist organizations.

Most of these newer businesses are collectively known as Money Service Businesses (MSB). Businesses that transmit money, issue money orders, cash checks, deal in foreign currencies, or a number of other types of transactions, are required to register with FinCEN and maintain an effective Anti-Money Laundering (AML) program.

We recently summarized a presentation FinCEN gave to the Secure Cash & Transport Industry last October. Alan Cox, Acting Associate Director of the Liaison Division for FinCEN, sent a very clear and powerful message to the industry: Comply with AML requirements or face significant enforcement actions.

Exemptions are Few and Far Between

Cox explained that the exemptions to FinCEN rules are extremely narrow, specifically with respect to currency transportation. A currency transporter can be exempted from FinCEN if it has ONLY a custodial interest in the currency or other valuable. But the conditions that define what is "custodial" are very limited and precise.

The Treasury and its implementing laws aim to throw a broad net over currency transactions, and use the resulting data in numerous legal investigations. Some recent FinCEN enforcement actions show that the agency defines MSB broadly, includes even small businesses, and takes punitive action when it deems a business is out of compliance:

- **B.A.K. Precious Metals, Inc.** received a civil money penalty of $200,000, December 2015: Failed to establish and maintain an effective AML program for its precious metals business despite repeated compliance reviews; failed to assess or monitor clients; failed to report transactions.

- **Oaks Card Club** received a civil money penalty of $650,000, December 2015: Failed to establish an effective AML program for its gambling business; alerted customers when they were about to pass the $10,000 threshold requiring a currency transaction report (CTR); failed to file suspicious activity reports (SARs).

Continued on Page 3

Not If But When: How to Avoid Becoming the Next Target of FinCEN AML Enforcement

Continued from Page 2

- **Lee's Snack Shop** received a civil money penalty of $60,000, June 2015: Failed to establish and maintain a compliance program; failed to conduct adequate testing; failed to file currency transaction reports.
- **King Mail & Wireless** received a civil money penalty of $12,000, June 2015: Failed to establish an effective AML program for its money wire transfer business; failed to file suspicious transaction reports.
- **Ripple Labs Inc.** received a civil money penalty of $700,000, May 2015: Failed to register as a Money Service Business; failed to establish an AML program for a virtual currency (Ripple); failed to file suspicious activity reports.
- **Aurora Sunmart Inc.** received a civil money penalty of $75,000, March 2015: Failed to re-register the check cashing service as an MSB on a timely basis; failed to establish an effective AML program; failed to report transactions over $10,000; failed to establish effective internal controls.

Businesses that transmit money, issue money orders, cash checks, deal in foreign currencies, or a number of other types of transactions, are required to register with FinCEN and maintain an effective Anti-Money Laundering (AML) program.

If there is even a remote chance that your business is a Money Service Business, look at the FinCEN requirements and determine if you should be registered with FinCEN. If your business is an MSB, you could face significant penalties for failure to comply.

Learn more about how to ensure your compliance by referencing our last article on this topic, "FinCEN's Alan Cox Foreshadows AML Enforcement Actions in Armored Car Industry Address".

The exemptions to FinCEN rules are extremely narrow, specifically with respect to currency transportation. FinCEN enforcement actions show that the agency defines MSB broadly, includes even small businesses, and take punitive action when it deems a business is out of compliance.

About The Author

Lowers Risk Group provides comprehensive enterprise risk management solutions to organizations operating in high-risk, highly-regulated environments and organizations that value risk mitigation. With Lowers Risk Group you can expect a strategic, focused approach to risk assessment, compliance, and mitigation to help drive your organization forward with confidence.

16 Fraud Facts to Fuel Your 2016 Prevention Planning

As we begin 2016, we thought it might be useful to get a quick big picture on organizational fraud for context. We have been posting about the causal factors driving fraud and urging you to develop an effective risk-based prevention program. Now, here's the why — 16 facts about fraud drawn from the 2014 ACFE Report to the Nations that should make it relevant to you.

1. Overall, survey participants estimated that organizations lose about 5% of top line revenue every year. That's $3.7 trillion in 2013 Gross World Product (GWP).
2. The median loss for a fraud episode was $145,000, but that conceals a wide variation in amounts. 22% of cases cost $1 million or more.
3. The median duration of a fraud — the length of time between inception and detection — was 18 months.
4. Asset misappropriation was the most common of the three types of fraud, occurring in 85% of reported cases and costing a median $130,000. The least common type was financial fraud at 9%, but these were extensive thefts with a median loss of $1 million. In between, corruption occurred in 37% of cases at a median cost of $200,000.
5. 30% of the reported frauds involved more than one type of fraud.
6. Over 40% of cases were finally detected through a tip, about half of which were from an employee.
7. Organizations with hotlines were more likely to uncover a fraud by a tip.
8. Organizations of all sizes and types experience fraud — for profit, not for profit, government, and in all industry sectors.
9. Smaller organizations suffer disproportionately larger losses than larger organizations.
10. Fraud varies by industry, with financial services, government, and manufacturing having the greatest number of cases, but with losses per case higher in mining, real estate, and oil and gas.
11. Anti-fraud controls work. Organizations reporting fraud that had these controls in place experienced smaller losses and shorter duration of a fraud episode.
12. Fraud occurs at all levels of the organization, including employees, managers, and owners/executives.
13. The more authority held by the fraudster, the greater the losses.
14. Collusion helps fraudsters evade controls. The losses from fraud schemes increased as the number of people involved increased.
15. Certain departments were reported as more susceptible to fraud — accounting, operations, sales, executive/upper management, customer service, purchasing, and finance.
16. Recovering losses was slow and uncertain. Only 14% of participants had recovered ALL losses, and 58% had recovered NONE at the time of the survey.

Request a meeting with a Lowers Risk Group consultant to find out more about how your organization can fight fraud.

ABA National Conference for Community Bankers
JW Marriott Desert Springs Resort & Spa — Palm Desert, CA
February 14-17, 2016

Learn how to achieve greater profitability in a high-risk environment at the premier event developed for – and by – community bank CEOs and senior level banking executives. This event will include sessions and speakers on topics such as interest rate risk, cybersecurity, non-interest income, industry issues and trends, legislative and regulatory updates, management strategies, the economy and more. More information on the conference may be found at www.aba.com.

D. Mark Lowers, CEO, Lowers Risk Group, will be speaking at the ABA National Conference for Community Bankers on **Monday, February 15th at 11:15 AM and 1:30 PM on the topic of Trust and the Art of Social Engineering.**