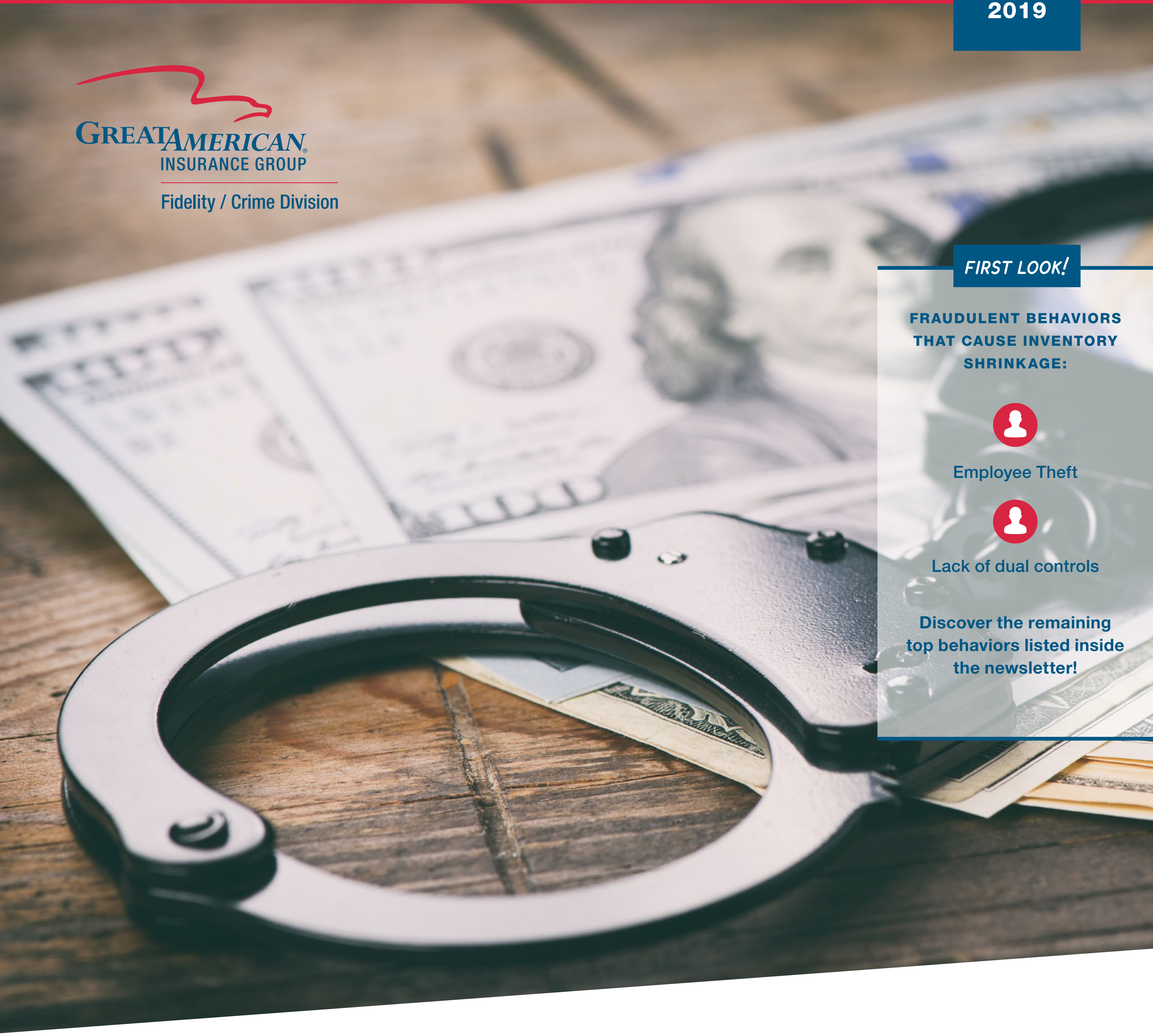
FALL
2019



GREAT AMERICAN INSURANCE GROUP
Fidelity / Crime Division

FIRST LOOK!

FRAUDULENT BEHAVIORS THAT CAUSE INVENTORY SHRINKAGE:

Employee Theft

Lack of dual controls

Discover the remaining top behaviors listed inside the newsletter!

INSIDE THIS ISSUE

The Crime Times

Blue Beaches Blue

Robert Larsen
Director
Fidelity / Crime Division

Bill Marston
Senior Vice President
Fidelity / Crime Division

For many years the Blue Beaches Condominium complex ran very smoothly and efficiently, but as time passed the quality of service deteriorated; the grounds looked terrible, streetlights were burned out, air conditioning repairs took weeks, and roof damage had gone unrepaired for up to three months. The entire Blue Beaches Condominium Association was fed up, leading to the Board of Directors to be voted out and a new board installed. The new board fired the Property Manager and most of the employees.

During the interview process the board managed the property until they were able to select a new manager. After interviewing eight prospective property management companies, they hired Total Management (TM). The board's decision was based on:

- Their impressions of the company during the interview
- The management plan the company submitted
- Enthusiastic recommendations of several nearby condo associations
- The company's financial standing
- Clean criminal records of the employees that would be involved with their property

Once TM was hired, they obtained a comprehensive power of attorney from the board. They set up two new bank accounts in the name of the Association, with themselves as signatories. The first account was an operating account for day-to-day expenses, and the other one was a reserve account for property taxes and extraordinary expenses. They arranged to collect all dues and assessments by automated clearing house (ACH) transfers into these accounts. They furnished the board with a detailed monthly statement showing operating payments, funds on hand, purchases and disbursements, and the individual account status of each of the 370 members. The statement was usually over 60 pages.

Within a couple of months conditions at Blue Beaches immediately improved. Even better, the monthly statements showed a significant savings in the operating expenses. The board and residents were very happy with TM.

Unfortunately, for the Board and the residents their joy did not last. TM was hired in January and in the following December two of the Association's employees complained they did not receive their paychecks for the current pay period. The board attempted to reach TM by phone with no luck. The board then contacted their bank and they were able to access the two accounts set up by TM. Surprisingly, both were empty. The bank found the money had been transferred to another TM account and upon further investigation they found this account was empty. The board then checked with two nearby associations and discovered they had also been victimized. The board reported the loss to the local Sheriff's Department who turned it over to the Secret Service a few days later. While the investigation was continuing, the board's crime insurance carrier was able to make a quick settlement. This enabled the Association to pay some of their outstanding bills. Unfortunately, for the Association their crime policy had relatively low limits and the net loss was in excess of $1,358,000.

When the board and their crime carrier compared the monthly statements furnished by TM to the bank statements, the statements proved to be complete fabrications. The board went to great lengths to hire an effective and honest property manager. However, had they taken the proper preventative steps, they would have been able to stop the loss or greatly lessen the impact to the Association.

IMPORTANT LESSONS TO LEARN FROM THIS THEFT INCLUDE:

- No HOA or Condominium Association should ever forgo receiving and reviewing monthly bank statements.
- Never give complete control of bank accounts to a management company or individual manager.
- Periodically check on day-to-day, and month-to-month activities of the manager.

INVENTORY LOSSES:

Fraudulent behaviors that cause inventory shrinkage:

- Employee theft
- False sales
- Manipulation of inventory records
- Lack of dual controls
- Creation of bogus shell companies.

Lack of controls that can cause inventory (hospital supplies and equipment) shrinkage:

- Lack of surveillance
- Zero monitoring of trash removal
- Nonexistent shipping and receiving controls
- Failure to segregate the duties on purchasing and receiving.

Joe Szary
Director
Fidelity / Crime Division
Olga Torres
Manager
Fidelity / Crime Division

Why are inventory controls keeping hospital administrators up at night?

Restless days, nerve-racking nights, zombie-like walks through sterile hallways. Having a loved one or family member in a hospital can be a very overwhelming experience. Now imagine you're the Risk Manager of that hospital, and fear your inventory controls aren't strong. You could wind up tossing and turning like a frazzled figure worrying about their loved one.

Selling stolen medical equipment can bring in big bucks. Preventing fraudsters from fleecing the hospital certainly keeps Risk Managers and Hospital Administrators up at night. Disappearance of physical objects through theft or misplacement reduces efficiency and increases the costs to hospitals and patients. While thefts of pharmaceuticals and insurance fraud are big issues in hospitals, this article focuses on a claim involving employee theft of a hospital's inventory.

If thieves regularly steal surgical supplies and equipment, hospital expenses rise which impact the hospital's bottom line. Further, rampant thefts could lead to equipment shortages, and in turn equipment shortages in an Emergency Room can harm patients and lead to traumatic results. Such inventory theft can be the "stuff of nightmares" to the Risk Manager and is usually the driver behind the type of inventory losses listed to the left.

One such employee theft ring went beyond the mere stealing of bandages and scalpels. The absence of any controls at a well-known hospital expanded inventory theft into the taking of wheelchairs, hospital beds, and operating tables.

How could these pieces of durable medical equipment just walk out the door? Well, let's continue our nightmarish tale by looking at Bob who's a longtime highly trusted and well-known employee. Bob has worked in the purchasing and receiving department for over 20 years. When hospital departments quickly need something, they go to Bob – even though they are not following the procedures laid out by the hospital. Bob's streamlined process increases the speed and efficiency of obtaining items and allows department heads to skip the hassle of completing requisition paperwork. Instead of requesting items through proper channels, a hospital department employee calls Bob, who does the following:

- Receives the order and completes the paperwork and orders the equipment.
- Sends all deliveries to his own attention, so he can verify the order is "correct" upon receipt.
- Expedites the order from the shipping dock to the department.

Is Bob just a trusted friend providing white-glove equipment requisition service to the department? Or, is this something more sinister? Unbeknownst to the department, Bob orders five operating tables, instead of the three operating tables requested by the department. Three for the department and two for Bob. Bob turns around and sells the two tables online for whatever price he can get for them. It's pure profit for Bob.

If the hospital enforced its ordering process, implemented a separation of duties between ordering and receiving, and verified all outgoing shipments, the hospital may have prevented the loss.

LET'S STOP AND REVIEW HOW THIS HAPPENED.

1. Various hospital departments didn't use the required ordering department to request supplies/equipment to allow for the proper tracking of orders.
2. Bob had exclusive control over the ordering process without any oversight.
3. He also controlled all aspects of receiving all supplies and equipment.
4. By holding the duties of shipping and receiving, Bob prevented the hospital from conducting a proper accounting of its inventory.
5. Bob's seniority and unrestricted dominion at the shipping and receiving dock allowed him to direct outgoing medical equipment onto trucks in route to Bob's buyers.

This hospital's nightmare resulted in two claims. The employee theft ring described above caused a loss of over $1.2 million. After the first loss, the hospital worked hard to revise and tighten up controls. Unfortunately, the creation and implementation of new controls took time during which the hospital suffered from another large Employee Theft claim amounting to approximately $275,000. We tell this tale to help you prevent similar losses. By increasing your purchasing controls and creating a segregation of duties, you may stop a similar loss from happening to you – thereby preventing a Risk Manager's nightmarish dream from developing into reality.

Defining the Risk of Cryptocurrency

LOWERS & ASSOCIATES (March 21, 2019)

The fundamental risk of cryptocurrency (‘crypto’), aside from market risks, is custody. Simply put, the high value of crypto, with the equivalent of over $100 billion in circulation (at this time), provides ample motivation to steal it.

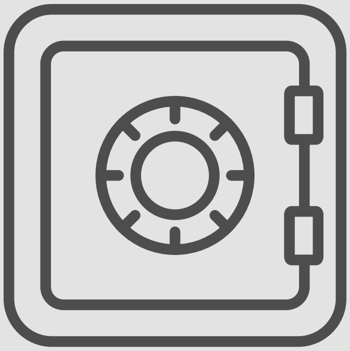
Hot vs. Cold Storage

Hot Storage

If the crypto is stored in a “hot” (online) environment, strong encryption is the essential safeguard, but the entire environment must be secured. The digital asset and the private encryption key that accesses it must be stored separately. Since the online account storing the asset is generally known to the public through the blockchain, the biggest risks are hacking attacks on the online storage or theft of the private key. Whoever holds the private key controls the asset. History has shown that online storage is highly vulnerable to theft.

Cold Storage

If the crypto or its private key is held in “cold” storage (offline)—as many experts recommend—then both digital and physical risks exist. As large and more traditional investors choose cryptocurrencies for value stores and transactions, the cold storage option is likely to increase. The need for strong encryption remains, and specific kinds of threats against digital assets, like electromagnetic radiation, must be mitigated.



That said, once the crypto and its private key are in the physical realm, many of the risks of crypto are like those that apply to compact high value objects like gems, bearer bonds and cash. A small cold storage "wallet"—a digital device that might be the size of a thumb drive—can hold and transfer any amount of cryptocurrency. These tiny devices are highly vulnerable to damage or theft, and even if a thief does not get the private key, they can still hold it for ransom.

A second major source of risk to crypto is the very reason it exists: it is outside of any traditional currency ecosystem, without the insurance and security protocols that accompany fiat currencies. No institution is monitoring crypto transactions, and no law enforcement agency is routinely tracking suspicious actors. In fact, the identities of investors in crypto may not be publicly known.

Financial institutions are beginning to evolve private ways to duplicate some of the protections of traditional currencies, like Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols. Cash in Transit providers are building on their experience in cash management to devise secure ways to store and transport crypto.

Crypto is still in the wild west phase. It is growing very rapidly, and a financial system is developing to make it a reasonable option to fiat currencies.

For more information about the risks of crypto, and how to manage them, request a copy of our new white paper Custodial Crypto Transportation and Storage: Understanding and Mitigating the Risks.

If you have questions, please contact:

DENNIS BURNS
dburns@gaig.com
(212) 513-4017

crimeinsurance.com

GREAT AMERICAN INSURANCE GROUP | Fidelity / Crime Division

301 E. Fourth St.
Cincinnati, OH 45202
800-545-4269
GAIG.com

Protecting hundreds of niche industries with **expert insurance** solutions.