

# JOURNAL OF ACCOUNTANCY

## FRAUD

### Lessons from an \$8 million fraud

## What the criminal was thinking and what can be done to prevent or uncover similar crimes

BY MARK J. NIGRINI, PH.D. AND NATHAN J. MUELLER  
AUGUST 2014



In hindsight, it seems obvious: Nathan J. Mueller's pilfering of financial services giant ING should have never been allowed to start, much less last as long as it did.

First, it was an accident that gave Mueller, an employee in ING's reinsurance division, the authority to approve company checks of up to \$250,000.

Then, the check his credit card company returned to ING could have exposed his theft in the first year, but the accounts payable department simply returned the check to him.

Finally, the evidence that he was living far beyond his means—the expensive cars and watches, the lavish nightlife, the frequent trips from Minnesota to Las Vegas—could have raised a few eyebrows among his co-workers, but nobody voiced any concerns for years.

In the end, Mueller embezzled nearly \$8.5 million from ING over four years and three months. When he was caught, he was sentenced to 97 months in prison—a term that he began in February 2009 at the Federal Prison Camp in Duluth, Minn.

Why should anyone care about Nathan J. Mueller? His case is noteworthy because of the millions of dollars involved and the length of time that his scheme went undetected and because his scheme was made possible by a breach of controls. This article describes the fraud in Mueller's own words and examines the lessons learned with strategies for management on how to prevent and detect similar schemes.

### THE PATH TO ING

Mueller grew up in a small town in south central Minnesota. A high school friend remembers that Mueller was popular in school, decent at athletics, and competent at his schoolwork, and that he liked to play rap music "pretty loud in his car" whenever he could. The friend also remembers that Mueller's family was always on a tight budget and that Mueller didn't like living that way.

Mueller attended a private liberal arts college and graduated with an accounting degree in 1996. He enjoyed the inner workings of accounting systems, and in 2000 he found himself part of ING after his employer, life insurance company ReliaStar, was acquired for more than \$6 billion.

Mueller played a lead role in transitioning his old employer onto a new enterprise resource planning (ERP) system. A mistake by his new employer created an opportunity for Mueller to steal company funds. In the next section of the article, Mueller describes the fraud scheme in his own words.

## **WE OFTEN LOGGED ON AS SOMEONE ELSE**

*As a part of the changeover team, I became an expert on all aspects of the ERP system including financial reporting, journal entries, and, most importantly, checks and wire payment processing. I was also, by mistake, along with a co-worker, given the authority to approve checks up to \$250,000. I discovered this permission quite by accident some two years after the takeover.*

*Our accounting department consisted of a controller, assistant controller, accounting manager (me), and three people under me. Together with a co-worker (CW) and a subordinate (SUB), I was one of three of us in my division who could request checks. CW and I also could approve checks. In our small accounting department, we knew everyone else's system passwords. This was a practical workaround for when we needed to get something done when someone was out of the office. We often logged on as someone else to get the job done. One morning, while sitting at my desk, I realized that I could log in as someone else, request a check, and then log in as myself and approve my own request. I went to work every day for the next year tempted by the pot of gold that was there for the taking.*

*In June 2003, my wife was pregnant and my annual \$80,000 salary was just not getting all of our bills and college loans paid. I thought that if I just paid off my debts, then we could do quite well with my income matching our living expenses. I tested my scheme by paying the current amount due on one of my credit cards that had a name that included the word "Universal." Just before I left the office late on a Monday afternoon, I logged on as CW and requested a check made out to Universal for \$1,100. This check looked normal because we did a lot of business with an insurance company that had Universal as the main part of its name. After the check was prepared, I mailed it with my statement to my credit card company, and the amount was applied to my account without a problem. For a while I felt guilty and worried. If I were caught, I'd lose my job for only \$1,100. Two weeks later, I decided to try it again, and my next check was for \$1,800. During that summer, I transferred all my other debt balances to the Universal card and kept requesting checks made out to Universal. After \$88,000 was paid against my credit card, I was free and clear of all debt, except for the mortgage on our house.*

*Just before I'd cleared all the charges to the Universal card, I noticed that one of my checks for \$4,500 had apparently gone missing. It wasn't posted against my credit card account, and it had not cleared the company's bank account. I was worried that something had caused the bank not to process the check or that my fraud had been discovered internally. For a few weeks I nervously looked at my emails each morning scanning the subject lines for words like "explanation requested." Each time the phone rang I assumed that I was going to be called upstairs for a meeting. Then at around 10 on a hot late-August morning, I received one of those brown interoffice recycled mail envelopes in my inbox from our accounts payable department in Atlanta. There was the check! I had forgotten to put my personal credit card number on the check, and so the card payment processors didn't know whose account to credit. They then mailed the check to the head office address. The accounts payable people also didn't know what to do with the check, so they sent it back to me, the check's requester. That stopped my 2003 fraud spree dead in its tracks.*

## **AFTER THE SCARE WORE OFF**

*By the middle of our bone-chilling winter, the effects of the scare had worn off, and I started thinking about how easy it was to get that \$88,000 "bonus." I couldn't help myself. I wanted to do it again, even though I didn't really need the money like before. I remembered the missing check scare, and so I now wanted a scheme that bypassed mailing the checks to my credit card company. I registered "Ace Business Consulting" with our secretary of state, got a federal ID number, and opened a bank account at a major bank with lots of branches in Minnesota. I chose Ace because our company did a lot of business with another company that had Ace in its name. On a Thursday afternoon, right before I left for the day, I logged on as SUB and requested a check made out for \$27,000. I then logged on as myself and approved it. I picked up the check on Friday and deposited it in Ace's bank account on Saturday morning. The teller treated the transaction like any other routine transaction and handed me the deposit receipt showing that the whole \$27,000 was available. I still remember her telling me to have a nice day. Using this method, I stole about \$1 million in 2004, \$2 million in 2005, \$4 million in 2006, and \$1 million in 2007.*

*Getting a check was easy because I logged on as CW or SUB and requested a check and then I approved the check. The checks were printed overnight, and it was SUB's job to collect the physical checks every day from the company building next door. I had to make sure that SUB had the day off the next day because, when SUB was away, I was the person who collected the checks. At my desk I would remove the Ace check from the batch, and all the other checks were mailed off to where they were supposed to go. Normally, I would just wait for SUB to take the day off, and I'd request an Ace check the day before. If I needed money urgently, I'd give SUB the day off so*

*that I could collect the checks.*

*For every credit (to the bank) there has to be a debit, and my debits needed to be hidden somewhere. Our payments were usually for insurance claims, commission expenses, various refunds, or an administrative expense. In 2003 and 2004, I hid all the debits in ledger accounts that had a lot of reconciliation activity, making sure that my debit helped the account reconcile to zero. One of my accounting tasks was to record the investment income of our Canadian investments in U.S. dollars (USD) in our U.S. accounting records. I was supposed to use the average Canadian-dollar-to-USD exchange rate to record the interest income. From 2005 to 2007, I would calculate the real exchange rate, and then I would purposely weaken the Canadian dollar by a few basis points to understate the USD value of that income. I was the only person who worked on this task for seven years, and because the accounting system had thousands of journal entries and billions of dollars of transactions, my Ace checks remained hidden.*

## **LET'S DO LUNCH SOMETIME**

*For every Ace check there was a deposit to my bank account, and I needed some explanation to spend my money without making my wife or my friends suspicious. In the beginning I told my wife, friends, and family that I was doing some accounting work on the side. At that time my lifestyle wasn't very different, and so the moonlighting explanation worked fine. When my lifestyle included high-end European cars, costly Las Vegas trips, extravagant watches, and expensive nightclub entertainment, I told people that I was an amazingly successful gambler and I got my extra income from hitting large jackpots on high-dollar slot machines. To do this, I would first wire money down to the casino in Las Vegas, and then I'd fly there (first class on Northwest). I'd then carry up to \$100,000 in cash back home at the end of the weekend with a stack of W-2Gs (which report gambling winnings). This gambling success explanation wasn't working all that well after two years and just under \$3 million in "winnings," and in June 2006 I knew that I had to choose between my wife and my fraud. It was either come clean to her about what I was doing or get away from her to insulate her from all the consequences coming my way. I knew I would eventually be caught, so I chose divorce.*

*By mid-2007, my fraud had cooled off, and I'd only taken \$1 million so far that year. An internal company review showed that three of us in accounting had check approval authorities, and we all received internal forms that needed to be completed. CW and I were talking about it with my boss in the hallway outside our offices one morning, and we all agreed that since we were all involved in the accounting function, we should not have the authority to approve checks. We actually revoked our own check approval authority.*

*CW and my ex-wife became friends while she and I worked together. At an afternoon lunch at Panera Bread in August 2007 they were (surprise!) talking about depressive, anti-social, hard-drinking, and overweight me. My ex-wife told CW that she didn't really believe the lucky-at-gambling explanation for my life in the fast lane. CW's suspicions were raised, and a few days later she ran a query to list all the 2007 checks that she had requested or approved. The results included 10 Ace checks adding up to \$1 million. At 2 p.m. on Friday, my boss asked me for the supporting vouchers for the Ace checks. I said that since SUB was off for the day, we should get to the bottom of things on Monday morning. Monday morning's meeting didn't go very well, and I literally ran out of the office. On Tuesday at 10:30 p.m., two of the company's fraud investigators rang the doorbell at my home in the exclusive suburbs of Minneapolis. It was an unpleasant conversation in which the word "Ace" was mentioned several times and ended only because I said that I wanted to talk with my attorney.*

## **AN OUNCE OF PREVENTION**

Organizations need an effective antifraud strategy to deter and detect employee fraud. These programs should include fraud prevention activities, proactive detection activities, fraud investigation activities (for suspected frauds), and the concluding civil remedies and criminal actions. Fraud investigations and obtaining civil remedies are very costly, and it is generally believed that prevention activities are the most economical way to control losses from fraud. Effective prevention activities usually involve maintaining an organizational culture of honesty and high ethical standards, assessing fraud risk, and reducing the opportunities to commit fraud. This section discusses the prevention activities that might have played a role in preventing the Mueller fraud.

An organization's *hiring policy* (where allowed by law) should include past employment verification, a background check, a credit check, and education verification. These policies and procedures should be applied in every hiring instance, including those in which groups of employees are onboarded as the result of a corporate entity acquisition.

Mueller found himself employed at a multinational company as a result of a takeover, effectively bypassing any screens that the company might have had in place. After a takeover, management should be aware that the incoming employees likely will have less loyalty to their new employer than the original employees have. The acquirer should carefully weigh its options when it comes to an assessment of fraud risk and give due consideration to the previously mentioned new hire procedures. Management also should consider subjecting the new employees to a modified, and possibly less strenuous, version of the new-hire procedures. In Mueller's case, a check of his credit report at that time would have shown that he was financially strapped and under real pressure for extra income, though that might not have been enough to disqualify him from receiving a job offer.

## IMPORTANCE OF ERP CONTROLS

The Mueller case is a good reminder of the importance of controls related to ERP systems. *Authentication controls* identify the person accessing the accounting system and ensure that only legitimate users can access the system. These controls include passwords, smart cards, and biometric identifiers. In Mueller's case, the authentication controls failed because he effectively impersonated either SUB or CW. His fraud could have been prevented if the company had used multifactor authentication, perhaps by requiring both a password and a smart card inserted into a card reader.

*Authorization controls* restrict the access of authenticated users to certain classes of information and capabilities. For two years, Mueller didn't even know that he had permission to approve checks. His approval limit of \$250,000 was also excessive. The ability to request and approve high-dollar checks, in part, facilitated the fraud.

*Processing controls* ensure that data is processed correctly and, by implication, that obvious errors are not processed. The Mueller fraud was made possible, in part, by the fact that he could keep his fraud concealed by posting the debits to a ledger account of his choosing (effectively journalizing his own fraud).

A control weakness related to *physical safeguards* was that the requesting and authorizing employees had access to the printed checks after they were printed. Employees who can request or approve payments should not have access to the printed checks. This control is also important in claims processing centers that, for example, process health insurance claims or tax refunds.

It is difficult to avoid the complexities and volume of transactions that come with being a multinational financial services company. Good business practices together with the risk of fraud provide suitable reasons to avoid situations where just one or two people understand the whole system and where one or two people are responsible for reconciliations and write-offs. Because Mueller could control the ledger accounts that were debited, he could keep his scheme undetected. This case shows the importance of the separation of operational responsibility from recordkeeping responsibilities.

The elements of the fraud triangle include pressure, opportunity, and rationalization. Extensive personal debts and a new child provided the pressure for the first phase of the fraud. As a fraud prevention measure, organizations should have *employee support programs* in place to assist employees struggling with addictions, mental and emotional health, and family and financial problems.

## A POUND OF CURE

The use of *forensic analytics* would have raised alerts with respect to the Ace vendor. Forensic analytics is the act of obtaining and analyzing electronic data using calculations and statistical techniques to reconstruct, detect, or otherwise support a claim of embezzlement or other financial fraud. The main steps in the process are data collection; data cleansing; running the analytics tests; and evaluation, investigation, and reporting.

The *largest subsets growth test* is based on the fact that people escalate their frauds at a much more rapid pace than what would be considered normal. They also don't know when to stop. A fraudulent vendor often shows explosive year-over-year growth. An employee using a company purchasing card for personal expenses often has geometric growth in total purchases. An employee with a fraudulent overtime scheme also often shows high growth in hourly totals, perhaps even to impossible levels. Running a computer-based test to review the vendors with the largest annual growth in total dollars would have shown that Ace's dollar growth was abnormally high and suspicious.

Mueller's lifestyle included expensive cars, trips, watches, and nighttime entertainment. People at work saw and

heard that he was living the high life. *Fraud awareness training* reminds employees at all levels in the organization that fraud is real and that it could be happening in their departments. A co-worker living beyond what his or her salary should allow is a classic red flag for fraud. "From early on, co-workers were aware of my trips to Vegas, my gambling, and my car," Mueller said. "As time went on, they would have noticed more and more things I had, and that should have sparked questions about where all my money was coming from." Had suspicions been raised as a result of fraud awareness training, this fraud could have been stopped as early as 2004.

It was a relatively simple query that highlighted the Ace checks. Mueller was eventually caught because of suspicions of fraud, but it was more due to a coincidence than anything else. Frauds are often discovered by tips, and to benefit from this detection avenue, organizations need to make available to employees an *anonymous fraud reporting channel*, such as a third-party hotline.

The fraud would have been discovered in 2003 if the accounts payable people had looked more closely at the \$4,500 check that was returned to them. A financial institution returned a check to the company saying that it didn't know what the payment was for. It should have seemed odd that a credit card company was being paid with a single check for a single account. One detection tactic would be to have all *abnormal interactions with outside parties* (e.g., errors, refunds, and overpayments) reviewed by a risk management person knowledgeable in financial matters so that remedial actions (including system changes) can be taken.

The fraud scheme used checks payable to Ace. While Mueller did not set up the vendor as a new vendor, companies need to carefully control who has permission to *add new vendors* to the payments system. Also, vendors that are dormant need to be deleted from the system to prevent employees who want to start a fraud from modifying an existing record instead of creating a new vendor.

## THE FINAL WORD

Mueller has paid back about \$860,000 of the money he stole, he said. Almost all of that has come in the form of assets—homes, cars, jewelry, and financial accounts—he gave directly to ING or that were forfeited by his ex-wife and friends, he said. He pays \$75 a month from prison through a repayment program.

With time off for good behavior and for completing the residential drug abuse program (for alcohol abuse), Mueller is scheduled to be released from prison in September. He will have spent a year and three months longer behind bars than he did stealing money from ING—a scheme that in hindsight should have never gotten started, much less lasted that long.

---

## EXECUTIVE SUMMARY

**A corporate mistake opened the door for Nathan J. Mueller's fraud.** Two years after the error was made, he discovered he was authorized to request and approve checks of up to \$250,000. A co-worker also was accidentally granted the same privileges, while a subordinate was authorized to request checks.

**Mueller, his subordinate, and the co-worker often logged on as one another to get work done.** This allowed Mueller to request checks under one identity and then approve them under his own account.

**Mueller and his subordinate were allowed to physically pick up checks.** This allowed Mueller to take physical checks to the bank to be deposited into the account of a fake vendor he set up.

**Mueller hid his debits in ledger accounts that he controlled.** Better separation of duties could have helped to prevent the scheme.

**The fraud netted nearly \$8.5 million in four years.** The money was used to buy expensive cars, watches, and nighttime entertainment as well as to pay for numerous trips from Minnesota to Las Vegas. Living beyond one's means is a classic red flag of possible fraud.

**Mueller told his wife his extra money was from gambling winnings.** After a while, she began to doubt that explanation, and they divorced.

**The fraud was uncovered when Mueller's ex-wife expressed her doubts about his income to his co-worker.** The co-worker spotted questionable transactions in the company records and brought them to management's attention. The scheme unraveled quickly after that.

**Mueller was sentenced to 97 months in federal prison after pleading guilty to fraud.** He is due to be released in September after 5½ years in prison.

**Mark J. Nigrini** ([mark\\_nigrini@msn.com](mailto:mark_nigrini@msn.com)) is an assistant professor at West Virginia University in Morgantown, W. Va. **Nathan J. Mueller** is an inmate at the Federal Prison Camp in Duluth, Minn. He can be reached starting in September at [nmueller@outlook.com](mailto:nmueller@outlook.com).

To comment on this article or to suggest an idea for another article, contact Jeff Drew, senior editor, at [jdrew@aicpa.org](mailto:jdrew@aicpa.org) or 919-402-4056.

---

## AICPA RESOURCES

### JofA articles

- ε "What's Your Fraud IQ?" Aug. 2014, page 38
- ε "What's Your Fraud IQ?" June 2014, page 40
- ε "What's Your Fraud IQ?" March 2014, page 46
- ε "What Gets Monitored Gets Detected," Feb. 2014, page 32
- ε "What's Your Fraud IQ?" Aug. 2013, page 26
- ε "Fraud Hotlines: Don't Miss That Call," Aug. 2013, page 32

### Publication

*The CPA's Handbook of Fraud and Commercial Crime Prevention* (#056504)

### CPE self-study

- ε Fundamentals of Forensic Accounting Certificate Program (#159950)
- ε Internal Control: Essentials for Financial Managers, Accountants, & Auditors (#731905, text; #181859, DVD/manual; #159821, on-demand)

### Conference

Forensic & Valuation Services Conference, Nov. 9–11, New Orleans

For more information or to make a purchase or register, go to [cpa2biz.com](http://cpa2biz.com) or call the Institute at 888-777-7077.

### Webpage

[FVS Fraud Resource Center](#)

## OTHER RESOURCES

### Publications

- ε *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*, by Mark J. Nigrini (John Wiley & Sons 2011)
- ε *Fraud Examination*, Fourth Edition, by W. Steve Albrecht, Chad O. Albrecht, Conan C. Albrecht, and Mark F.

Zimbelman (South-Western Cengage Learning 2012)  
Association of Certified Fraud Examiners (ACFE), 2014 *Report to the Nations on Occupational Fraud and Abuse*, [acfe.com/rtn-download-2014.aspx](http://acfe.com/rtn-download-2014.aspx)

### Practice tool

[ACFE Fraud Risk Assessment tool](#)

---

Copyright © 2013 American Institute of Certified Public Accountants. All rights reserved.