FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

WHITE-COLLAR crimes

By Lisa A. Tyler
National Escrow Administrator

In the May 2013 edition we shared a story entitled "SUSPICIOUS co-worker uncovers defalcation" containing the details of a former employee who wrote more than 40 checks to herself, before a co-worker in the accounting department received a call from a credit card company about a check received with no name on it.

The thief overheard the call and immediately took the paperwork into her office, and the co-worker ultimately reported the suspicious activity to her boss. We soon discovered the employee stole almost $650,000 from the escrow trust account over a seven-year period. Now we are sharing the results of her sentencing in the story entitled "THIEF failed to pay income tax."

Cyber thieves strike Fidelity's Albuquerque operation and duplicate an outgoing wire transfer and steal more than $100,000! Read the story entitled "ALTERED outgoing wire" to discover the details and to make sure your operation has all the preventative measures in place to ensure this type of crime does not happen again.

A contractor and home builder thought he was doing everything right – he purchased a lot, built his dream home and then tried to pull out cash with a new loan. Then he found out the title examiner discovered a lien on the property. Read the story entitled "MULTI-MILLION dollar judgment" to find out what happened when the escrow officer had to deliver the bad news to the homeowner.

SAFETY CORNER provides helpful information to keep you safe while you are "USING an automated teller machine (ATM)." Read the story to discover how to keep yourself safe from financial and physical harm while accessing your money.

IN THIS ISSUE

Share Fraud Insights
via email, mail or word of mouth.

volume 8 issue 10
October 2013

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

TELL US HOW YOU
STOPPED FRAUD

settlement@fnf.com or
949.622.4425

THIEF *failed to pay income tax*

How do you bring the federal government into a white-collar crime case? Report the thief's ill-gotten gain to the Internal Revenue Service (IRS). It is brilliant! The IRS hunts down the thief for failing to properly file a tax return and pay income tax on the stolen funds.

Laurie Brezinski, 43, of Schererville, Ind., pled guilty to the charge of, "…embezzlement of more than $5,000 from a corporation engaged in the business of insurance." She was sentenced by a District Judge to 37 months imprisonment; she must pay $659,048.63 in restitution to Ticor Title Insurance Company and serve two years of supervised release. The conditions of the supervised release include the following:

1. The defendant shall not seek or maintain employment that includes unsupervised financial or fiduciary-related duties, without the prior approval of the probation officer.
2. The defendant shall not participate in any form of gambling or patronize any gambling facilities (she claimed she had a gambling problem which caused her to steal money).
3. The defendant shall not incur new credit charges or open additional lines of credit without the approval of the probation officer unless the defendant is in compliance with the installment payment schedule.
4. The defendant shall provide the probation officer with access to any requested financial information.
5. The defendant shall participate in a mental health treatment program and shall abide by all program requirements and restrictions.

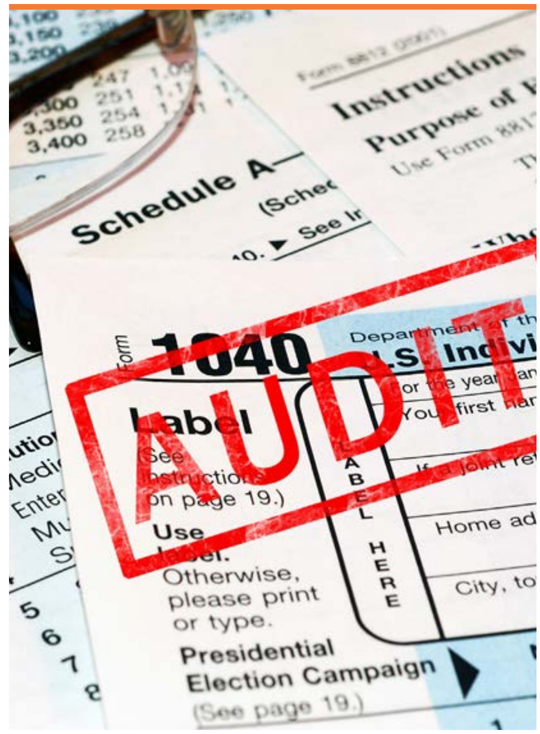
Along with pleading guilty to the theft, she also pled guilty to lying on her income taxes by hiding her criminal profits! She now owes the government about $180,000. This case was the result of an investigation by the IRS and was prosecuted by the Assistant United States Attorney.

Some of the evidence against Brezinski that led to the 37 month sentence was presented in court and showed her continued criminal activity even after being caught. The evidence included the fact she conspired with her next employer (after Ticor) to have her overtime earnings paid to her husband in order to avoid garnishment, since Ticor won a monetary judgment against her in a separate previous civil case.

Other evidence showed that while employed at Ticor not only did she write checks to herself, she schemed to double her money during a refinance of her home. She took out an equity loan for $57,000, cashed the loan proceeds check and then claimed she lost the check.

Brezinski covered her tracks by making it appear in the system the first check had been cancelled, so the settlement agent wrote her a second check, which she also cashed.

At the sentencing her former boss told the judge, "As bad as the theft was, it was her breach of trust that rocks us even more." The judge responded by saying, "Ms. Brezinski is a thief, pure and simple," adding that, "…white-collar crimes are no better than any other crime."



MORAL OF THE STORY

The Company will prosecute theft to the fullest extent of the law. To make sure the stolen funds are eventually fully repaid and Brezinski never works for our Companies in the title industry again the Company took the following steps:

- **Terminated the employee**
- **Reported her to the local authorities**
- **Reported her criminal actions to the IRS**
- **Prosecuted her in civil court to win a judgment lien to collect full restitution**

Thirteen Company representatives attended the sentencing. During the sentencing the manager of the Ticor operation testified to the Company's financial losses. The operation was forced to lay off and furlough some employees, and cut the wages of others to make up for the loss the operation endured having to replace the stolen funds.

ALTERED outgoing wire

In New Mexico an outgoing wire transfer form was sent to the accounting center to process and send seller proceeds on a Tuesday. It never got there. Three days later the same wire transfer form was sent via email to the accounting center, but this time the form was altered and the wire amount more than doubled!

Somehow the initial outgoing wire transfer authorization was intercepted after it was processed by the accounting center. The following information had been altered:

- Settlement date
- Transaction date
- Trust accounting date
- Payee name
- Amount
- ABA routing number
- Credit account name
- Credit account number

The initial wire transfer sent on a Tuesday represented seller proceeds in the amount of $47,848.60. The fraudulent wire transfer sent on Friday was $105,075. The accounting center ran the outgoing wires report on that same Friday from their production system after releasing all the wires that day.

They compared the report total to the total shown on their wires bulletin board, which is done each day to make sure the totals match. The accounting center wants to ensure they have processed all posted wires for the day and that the escrow branches did not forget to transmit any outgoing wire forms, as they are busy.

That day, the amount of outgoing funds on the wires bulletin board exceeded the balance on the report. The $105,075 wire showed as processed on the wires bulletin board, but was never posted as a valid wire on the production system. They immediately tried to recall the wire only to discover the entire amount had already been drained by the account holder.

The accounting center contacted their state manager who in turn notified the team in the National Escrow Administration Department. The administrators located the account holder in Philadelphia and contacted him to return the money. He explained the funds were sent to him on behalf of his business partner.

When he originally went to the bank, the branch did not have enough cash on hand, so he only withdrew $50,000. He then drove to the next branch and withdrew the balance of $55,075. He supposedly turned the cash over to his business partner to pay entertainers for an event they were hosting over the weekend. He said he did not realize the money had been stolen and promised to contact his business partner to return the funds.

In the meantime, the Company contacted the Albuquerque Police Department, the Philadelphia Police Department and the Secret Service to report the theft. The Secret Service agent assigned to the case acted swiftly in hauling the bank account holder into his office for questioning. During the questioning, the bank account holder agreed to allow the officer to monitor a call to his business partner to plea for a return of the funds. On the call the partner admitted sending the stolen funds to Nigeria!

Although law enforcement and others are still pursuing the case, it is not likely the Company will recover the funds. We have filed a loss for the $105,075. Not only that, we had to notify the sellers their bank account information had been exposed to the crooks when we sent their proceeds via wire transfer. We agreed to provide them a year's worth of Credit Check Basic® through Experian® and notified them of the importance of closing their account at the bank.

MORAL OF THE STORY

The policy for any accounting center personnel initiating and approving wire transfers using online banking software, is to use designated terminals equipped with Citrix® to prevent someone from hacking into their workstation, miming their keystrokes and then accessing our trust accounts. These specially designated terminals prevent our Company from becoming a victim of cyber theft. The New Mexico accounting center is now using workstations equipped with Citrix®.

In addition, accounting centers will now balance their outgoing wires report to their wires bulletin board constantly throughout the day. They will verify every outgoing wire form posted by the escrow branches in the escrow production system, before initiating and releasing each outgoing wire.

They will also change the passwords to their generic email accounts where outgoing wire transfer forms are sent by the escrow branches to make sure they are keeping their emails secure.

MULTI-MILLION dollar judgment

A contractor bought a vacant lot in Winter Park, Fla. with cash and built a $1.4 million home. The contractor went to his local bank to obtain a $1 million loan after he completed building his dream home. Fidelity was then asked to insure the $1 million loan. The title examiner for the order found a multi-million dollar judgment in the chain of title and brought it to the attention of the escrow officer before sending the completed commitment.

Here is what happened: In 2008, a lender lent $650,000 to a real-estate developer (developer) using the vacant two-acre lot on a lake as collateral. The developer had been a successful homebuilder and developer, whose companies were responsible for a pair of high-end 18-story condominiums in Orlando, Fla. that later went bankrupt.

The developer also had financial problems in Volusia County, Fla. where in 2011, a judge entered a $12.6 million judgment against him because of a failed $20 million Daytona Beach hotel redevelopment that resulted in foreclosure and a courthouse auction.

That judgment was recorded as a lien in Orange County, Fla. on January 18, 2011. One month later, the lender took the title to the vacant land in exchange for forgiving the $650,000 debt. Four months later, the lender sold the land in the upscale Winter Park subdivision to the contractor for $760,000.

The lender did the legal paperwork in both transactions – the swap with the developer of the mortgage for the deed, and the sale to the contractor. In that sale, the lender signed an

[Continued on pg 4]

[MULTI-MILLION dollar judgment – continued]

affidavit - which had been prepared by his son - declaring that there were no judgments or liens that encumbered the property.

The contractor then built a $1.4 million, 8,500-square-foot home on the lot in 2012. According to Orange County property records, the land and home are worth $2.2 million. At the time of purchase, the contractor received an owner's policy of title insurance from one of Fidelity's biggest competitors, but only for the value of the vacant land, $760,000.

After completion of construction, the contractor went to a local bank to borrow $1 million against the property. The bank opened an escrow with Elizabeth Fierro, an escrow officer with Fidelity's Lenders Express Division in Tampa. Elizabeth placed the title order. The title examiner assigned by Property Insight was Richard Mirabella, an outside vendor.

Richard informed Elizabeth of the $12.6 million judgment attached to the former owner and the property. Elizabeth reached out to the title insurance company who had insured the lot purchase for a letter of indemnity against the multi-million judgment and later received the letter.

Elizabeth and her underwriter reviewed the letter of indemnity, and together they determined the letter did not contain sufficient language to protect the Company from a future claim or loss. Elizabeth declined to close and insure the $1 million loan. Her manager said, "Elizabeth is sharp enough to know occasionally there is a valid reason to say 'no' to a customer."

The contractor says he wants to sell the property and be done with the whole mess. He has brought a lawsuit against the former owners of the property. In the meantime, if he sells the home, he will get none of the money. Instead, it will go to pay off the lien holder that won the $12.6 million judgment against the developer in Volusia County.

The contractor also has a claim against his original title insurance company, but the policy limits of $760,000 are not nearly enough to reimburse the $1.4 in construction costs and the judgment lien in the amount of $12.6 million.

Richard Mirabella and Elizabeth Fierro were rewarded $1,000 for their joint efforts. Richard received his half for searching and discovering the judgment lien against the former owner. Elizabeth received her half for obtaining the indemnity letter, working with her underwriter to determine it did not contain sufficient language to mitigate our risks on a $1 million policy of title insurance, and for telling the customer we would not close and insure the loan.

MORAL OF THE STORY

A judgment against a debtor can be recorded as a lien in any Florida county. Once that happens, proceeds from any property sale by the debtor in that county would go first to pay off the lien holder. Somebody apparently missed that judgment lien in a previous title search and now the property is encumbered until the judgment lien is satisfied and released.

Had we closed and insured the $1 million loan it would have been in second lien position behind the judgment lien. The lienholder would have had a priority lien position adversely affecting the proposed insured lender's ability to foreclose on the property had the borrower failed to make their agreed upon payments.

USING an automated teller machine (ATM)

SAFETY CORNER is dedicated to providing you with tips for being safe in your personal life.

Many of us are accustomed to the convenience of ATMs. This month's tip will serve as a reminder of how to use ATMs safely.

1. Stay alert. Choose ATMs located in well-lit areas. Do not use an ATM which is near shrubbery or at the corner of a building since corners create a blind spot. Be aware of your surroundings such as people standing behind you or anyone sitting in a parked car nearby. Cover the key pad when entering your Personal Identification Number (PIN). When using a drive-up ATM, be sure to keep your engine running, all doors locked and windows up, both before and after the transaction. When leaving an ATM make sure you are not being followed. If you are, drive immediately to a police or fire station, or to a crowded, well-lit location or business.
2. Be prepared. Complete all paperwork in advance. When you have completed your transaction, do not count your cash out in the open and be sure to put your card away immediately. Never count cash at the machine or in public. Wait until you are in your car or another secure place.
3. Walk away. Do not use an ATM that appears unusual looking or offers options with which you are not familiar or comfortable. Do not re-enter your PIN if the ATM eats your card, instead contact a bank official. If you notice anything suspicious use another ATM. There are devices which fraudsters attach over the card slots for "skimming" or gathering information from the magnetic strip on the back of the card, or they use transparent overlays on ATM keypads and tiny cameras hidden behind innocent-looking brochure holders, focused on where ATM users enter their PINs.
4. Keep your receipt. It serves as a record of your transaction. Be sure to review your statements against the receipt and look for any other irregular or fraudulent activity. Your liability for unauthorized transactions depends on how quickly you report the loss. You risk unlimited loss if you fail to report timely.

Statistics show more men are attacked at walk-up ATMs. Women are attacked at drive-up ATMs. If you are confronted by someone demanding your money give it to them. Your safety is of overall importance.

SAFETY CORNER