FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

# CAUGHT red-handed

By Lisa A. Tyler
*National Escrow Administrator*

"Where there is a will, there is a way" is a saying meant to inspire someone to higher achievement. Unfortunately, it applies just as easily to motivate a thief! Read the story about a desperate identity thief who was caught red-handed with stolen escrow documents in the story titled "OFF-SITE shredding is dangerous." The story provides some helpful hints about using a National Association for Information Destruction (NAID) certified shredding vendor.

Read "TAKING photos of identification" to discover how a mobile signing agent exposed borrowers to identity theft by snapping pictures of their identification and then transmitting the photos back to the office.

The borrowers in this story had every right to be angry with the signing agent (as well as our Company) since our employees selected and arranged for the signing agent to meet with them. In this story you can also discover methods of securing borrowers' non-public information, this story is especially important to those readers who are commissioned notaries.

"FREAKY friday" features a mix-up of gigantic proportions. Read the story to discover how two buyers of two different properties had their non-public personal information delivered to the wrong closing.

The story serves as a great lesson to all settlement agents to double-check document copies before delivering them to the consumer to ensure they are the documents they were intended to receive.

SAFETY CORNER provides helpful information to keep you safe while you are in your home. Read "GARAGE door safety" to learn how accessible your home might be to crooks that use garage door openers to break into homes.

## IN THIS ISSUE




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

volume 8 issue 9
September 2013

# FRAUD Insights

**Publisher**
Fidelity National Financial

**Editor**
Lisa A. Tyler
*National Escrow Administrator*

# OFF-SITE shredding is dangerous

**Recently an escrow office was contacted by local law enforcement to come to the police station to pick up documents with the office's contact information on them. Law enforcement stated the documents appeared to be thrown out in the trash, but had instead been found in a bag in the backseat of a suspected criminal.**

The manager received more details from the police officer when she arrived at the station. The police arrested a woman they had been investigating in connection with reported identity theft. Upon arrest, the police found a shredding bag of documents in her back seat from both the escrow office and from other sources. The documents from the escrow office were dated two weeks prior.

Apparently, the woman stole or purchased the documents from the off-site shredding company prior to them being shredded. The manager picked up the documents and returned to her office to comb through them.

The office personnel sent a notice of security breach to each consumer whose information had been exposed in the crime along with a coupon good for two redemptions of CreditCheck® Basic through Experian®. The office then terminated their relationship with the off-site shredding company and immediately hired an on-site shredding company.

In other related news…another office had their shred bins emptied by an off-site shredding company. The shredding company employees entered the office, removed the bins, emptied them into their truck and then placed the bins back in the office.

As they were pulling out of the parking lot, the National Escrow Administrator happened to be following them. To her amazement when the shredding truck pulled out into the street, the back door swung open and it began raining documents on the street.

The escrow administrator had to make some daring maneuvers to pull the shredding truck to the side of the road to tell them to lock the back door of their truck – and more importantly - to collect the hundreds of documents all over the street.

Unfortunately, on-site shredding does not offer a complete solution. There have been incidents with on-site shredding vendors too. One vendor lost documents when a big wind picked up, because its employees were not shredding in a secure facility.

The Company has contracted with approved shredding vendors that maintain a NAID certification (National Association for Information Destruction). Part of the certification process includes tracking the "chain of custody" of documents to be destroyed.

For instance, when the Company destroys boxes at a FNF Record Center, they cannot possibly destroy 200,000 boxes on-site. The approved shredding vendors bring their trucks to our facility for loading. Upon leaving, they close, lock and take a picture of the back doors. They can also show us when the truck arrives to their locked, secure facility where the shredding occurs. Done properly, off-site shredding can be just as safe as on-site shredding.

If your operation is utilizing a shredding vendor that has not been approved by the Company and/or is not NAID certified, it is important you terminate the contract and engage in the use of one of the Company's national vendors.

You can find more information about them at home.fnf.com

- Business Tools
- Purchasing at the **FNF Purchasing Store** under **Services**

Or you can contact your national escrow administrators for more information at settlement@fnf.com or at 949.622.4425.

# **TAKING** photos of identification

**In the March 2006 edition of *Fraud Insights*, there was a story titled, "I have finally found a worthwhile use for my camera phone!" The article was about settlement employees who were performing signing services outside of the office.**

The employees reported using their cell phones to capture a picture of the identification borrowers presented at signing. This practice was initiated in order to satisfy lender requirements to obtain proof of identification in compliance with the Patriot Act. The employees emailed the pictures from their phone to their desktop to print and provide to the lender.

Fast forward to 2013 where we have the same scenario, except the signing agent is a mobile notary and not an employee of the Company. The signing agent meets with the borrowers on a new loan, asks for identification and makes a journal entry. The signing agent snaps a picture of each driver's license, then returns them to the borrowers and proceeds with the signing.

In this case, the borrowers grew concerned about having their identification photographed, and called their escrow officer at Chicago Title Company to find out why the signing agent took a picture of their identification. The escrow officer checked the loan instructions and it did not require a copy of the borrowers' identification at signing.

The escrow officer called the signing agent and asked why photos were taken of the licenses. The signing agent confirmed the licenses were emailed along with an invoice for the signing appointment to the owner of the mobile signing company, which was a standard operating procedure.

The escrow officer then asked the signing agent if any email encryption software was used to protect the identification of the borrowers in the email transaction. The signing agent did not use email encryption software.

The escrow officer asked if the mobile device itself contained encryption software so the pictures and other data could not be accessed in the event the phone was lost or stolen. The signing agent said it did not.

The escrow officer realized the seriousness of the situation. First, the signing agent exposed the borrowers' non-public personal information over the Internet without encryption, so anyone with access to the Internet would have the ability to intercept the message and view its contents.

Second, the signing agent continued to store the photographs on an unencrypted cellular phone that could have been lost or stolen, thereby exposing the non-public personal information of the borrowers to anyone who might pick up the device.

The escrow officer demanded the photos be immediately deleted from the signing agent's phone and Sent items in the email account. She notified the owner of the signing service company of the signing agent's actions and demanded any photographs of the borrowers' licenses also be deleted from the agent's email account.

Then the escrow officer called the borrowers and explained why the signing agent took photos of the licenses, the measures that had been taken, and offered the borrowers a year's worth of CreditCheck® Basic through Experian®.

She also offered them a coupon worth two redemptions of credit monitoring through Experian® so if their identities or their credit are compromised as a result of the signing agent's actions, they will be notified by Experian® and their fraud resolution team will work to resolve any issues.

What if an employee of our Company had been performing the signing and did not have a Company issued cell phone? If the employee is sending photos and other information from a cellular device that is not Company issued, the email encryption likely will not work.

Employees cannot send a photo of an identification card - even to themselves - if the email cannot be encrypted since its contents would potentially be exposed to anyone on the Internet.

If employees have a company issued cell phone, they can send an encrypted email simply by typing the word {encrypt} in the subject line of the email message.

Additionally, unless the device itself contains encryption software, the employee's phone should never contain Company or consumer private information. Company issued cellular phones can be remotely encrypted if they are ever lost or stolen to avoid exposing Company or consumer non-public information.

FRAUD Insights

# FREAKY friday

**Two buyers of two different properties on two separate transactions equal one big nightmare for an escrow branch! Two buyers were signing their closing documents (including documents for their purchase money loans) with two different closers on a Friday afternoon. The closers took their packages to the copy room to run executed copies for the buyers before they left the office.**

The copies were delivered back to the buyers and they each left the office with documents in hand. The closers packaged up the original documents and prepared to send the loan packages to the lender for funding. After 5 p.m., everyone left the office for a great summer weekend.

On Monday morning one of the buyers called her closer to inform her that the document copies she and her husband received at closing were not theirs! The closer asked the buyers whose copies they had in their possession. She asked them to bring the copies back to the office.

In the meantime the closer scrambled to find out who had HER buyers' copies. She looked in the system to determine the names of the other buyers who were in the office on the same day and their assigned closer. She approached her co-worker about the problem and her theory that the document copies were switched in the copy room.

Her colleague was shocked that this could happen and placed a call to the buyers on the transaction she closed. The buyers pulled out their documents copies and sure enough they had the other buyers' copies. They agreed to bring them back to the office.

The document packages each contained not only transactional information, but the buyer's loan applications with bank account and credit card information. After realizing they had just compromised the identity and credit of each buyer, the two closers contacted their National Escrow Administrators who provided them with directions on how to proceed.

When each buyer arrived with their copies the closers sat down with them and apologized profusely for the mix-up. They provided each buyer with the correct set of document copies, as well as a year's worth of Credit Check Basic® thru Experian® and a check to reimburse them $110 for a twelve-month LifeLock® subscription.

After the respective buyers left the office, the office staff held a meeting to discuss the mix-up and to ensure that measures were put in place to prevent the same mistake from happening in the future.

# GARAGE door safety

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

Many people have homes with a garage and an automatic garage door opener. Having a garage door often gives people a false sense of security. Garage doors can be easily opened by thieves looking to steal items found in your garage or even worse, your home.

Keep in mind that garage door openers work off of a frequency that might enable someone else with a garage door opener on the same frequency to open your garage door. Then they can close the garage door, enabling them to load up their vehicle with items they find in your garage.

In some cases, you might be able to turn the automatic door opener off when you come home. Look on the remote control nearest your door to see if it has an off switch. If it does, turn it off while you are in your home for added security. When you leave, you can turn it back on for easy access.

Is the door from your garage into your house as secure as your front door? Ensure you have a strong, sturdy door with a deadbolt on it. Be sure to lock the door just as you would your front door. It is important to think of your garage as a shelter for your vehicle and not an extension of your living space.