FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

FAST grab for identity thief

By Lisa A. Tyler
National Escrow Administrator

Take a look around your office. What would a thief take if he broke in? We have learned in previous editions, they would likely take a document safe not bolted to the floor. You would think they would most likely take computers too, right? Wrong! Read the article entitled "PAPERLESS?" to find out what is most valuable to a thief these days.

We learned in the May 2012 edition that settlement agents should not send copies of earnest money checks disclosing buyer's bank account numbers to an unauthorized person (i.e. listing agent, seller, seller's attorney, etc.). Read the story "EXPOSED" to discover why the buyer's bank account information should be protected as highly as all other non-public, personal information. The MORAL OF THE STORY contains details on how to secure banking information included on checks received into escrow.

The industry is under attack by cyber-fraud, where funds are diverted out of an escrow trust account by hackers that are able to mime keystrokes from an employee's workstation and access the account online. The latest stories regarding this crime all involve independent escrow companies. Read "DIVERTED funds" to find out what happened to an independent escrow company who had this crime perpetrated against them.

Be sure to read the latest "SAFETY CORNER" tip surrounding the use of Company-issued laptops and tablets.

IN THIS ISSUE

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

volume 8 issue 6
June 2013

PAPERLESS?

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

One escrow office learned too late how important the Company's position is with regard to going paperless. The staff left the office late one evening. The cleaning crew finished around midnight and left the building. At 6:45 a.m. the next morning a neighboring tenant arrived and discovered rocks had been thrown through the glass doors of the Chicago Title office!

The neighboring tenant contacted the branch manager with the bad news. The branch manager rushed to the office and surveyed the damage. She immediately contacted the county manager, building manager and the police.

She found the glass doors broken and expected computers and the new flat screen television to be a part of the missing property. She was wrong! The only items missing were escrow files and one file containing copies of their daily deposits. As soon as the office staff arrived they began inventorying and recreating the missing files.

The office discovered 28 files were missing: 16 open, 9 closed and 3 cancelled. The staff quickly got to work sending out letters to the principals in all 28 transactions, making them aware of the security breach. They also contacted clients whose checks were included in the deposit file for the day.

They provided each principal with a coupon worth one year of CreditCheck® Basic through Experian®, which monitors their credit and notifies them if it is compromised. The notice of security breach encouraged principals' whose banking information was exposed to immediately contact their bank and tell them their account might have been compromised to prevent unauthorized access and fraudulent activity on their account.

Only one file had a Company issued, un-cashed check. The check was in the amount of $14.59 but was voided and reissued. The void eliminated the Positive Pay™ record at the bank, so the first check could never be cashed by the thieves.

Our Company takes the security of our customers' information seriously. The office has a security alarm, but it did not sound. A technician from the security company came out to test the alarm and could not determine why the system failed.

The motion detector for the side of the office the intruder was in did not activate. The alarm was set and when the staff stepped into the opposite side of the office, the alarm immediately went off. The manager sent a notice to the alarm company informing them they would be discontinuing service and using another provider.

MORAL OF THE STORY

The staff should not have entered the office until the police arrived. The criminal could have still been in the office and harmed the employees.

Waiting outside for the police to arrive would have provided the police with the ability to fingerprint doors and desks to see if this criminal was already in their database.

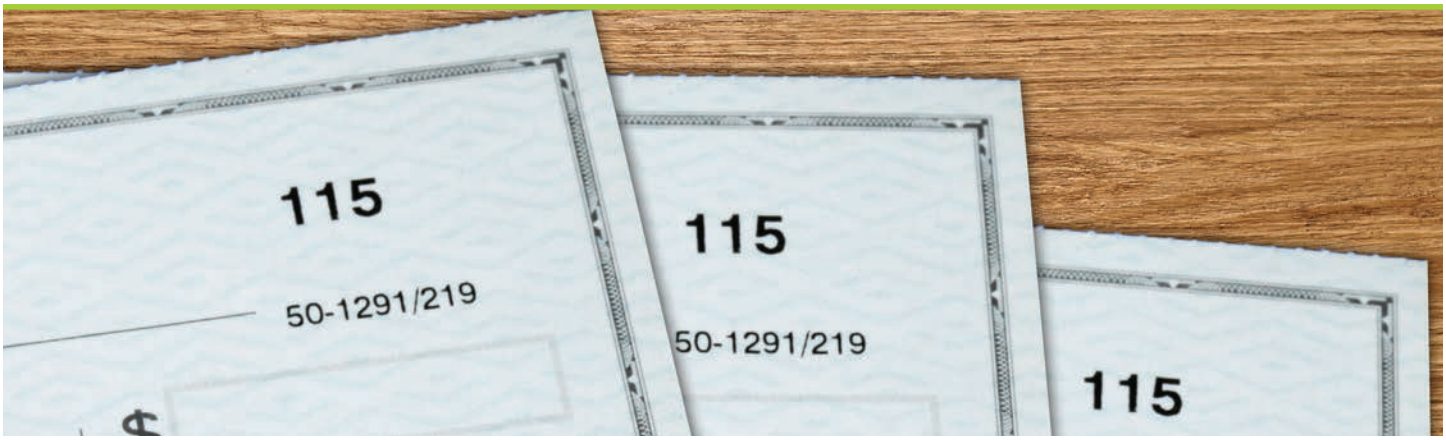
This particular office was converted to smartVIEW more than a year ago and trained to create electronic files instead of paper files to secure customer data and to increase efficiencies in their office. There are many benefits to smartVIEW, and one of them is the ability to eliminate paper files which results in eliminating the risk of a security breach such as the one in this story.

The staff failed to embrace the smartVIEW system and to create electronic files rather than paper files. If all the files were properly uploaded into smartVIEW there would have been no files for the thieves to grab and run with. In addition, smartVIEW files are not stored on a computer hard drive. Instead, the information is stored on a server. Therefore, even if a computer was stolen the criminals still would not be able to access the electronic files.

STOP

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425



EXPOSED

It is normal and customary practice at most escrow branches to make a photocopy of the earnest money check at the bottom of the system-issued receipt and provide a copy of it to the listing agent, selling agent, mortgage broker and lender.

In one escrow branch they did just that, only to find out from the buyers the information from the earnest money check had been intercepted by fraudsters who attempted to write more checks using the same exact check number in various amounts to different payees.

In February 2013, the buyers wrote a check to Chicago Title Company in the amount of $18,450 as an earnest money deposit on a new house. The check was receipted by the escrow branch, copied at the bottom of the receipt and then sent via unencrypted email to all parties.

Five days later, the buyers' bank contacted them as several checks bearing the same account number and same check number (6725) were presented at the bank for payment to different payees, all in large amounts. In addition, the bank told the buyers their online account had been threatened, and it was important they come to the bank to close the account and open a new one.

The buyers were furious and were convinced their account was compromised due to the actions of Chicago Title Company. Chicago Title Company reacted swiftly to the allegations they had anything to do with the exposure of the bank account information by providing the buyer with a free year's worth of CreditCheck® Basic through Experian®.

The buyers were not satisfied with the gesture, as they spent many hours and phone calls to change account numbers on their online payments (including four hours at their bank and 10 hours following up with creditors). The buyers demanded a full refund of their escrow and title charges.

Chicago Title might not have been the source of the theft, but they did expose the account information over the Internet by transmitting unencrypted emails containing copies of the check to parties entitled (and un-entitled) to the account information.

The escrow operations manager answered the buyers' demand for a refund of fees, letting them know fees cannot be discounted or waived in their state. They have to be collected in accordance with the rates filed with the State's Department of Insurance. The escrow manager requested a time and effort report reflecting the time expended by the buyers to change their compromised account, including any and all bank expenses.

The buyers provided letters from their employers and their bank verifying loss of work hours and production. The husband's employer reported the husband was unable to work for a total of 12 hours while dealing with financial issues brought on after his escrow with Chicago Title Company. The employer went further to report that based on the husband's salary and commission he would have earned close to $1,600 during the absence.

The wife is a dental hygienist. Her employer reported she was unable to work for 12 hours while dealing with financial issues as a result of their escrow transaction with Chicago Title Company. The employer estimated a loss of wages in the amount of $1,000.

The buyers' bank substantiated the loss of time by reporting that they spent several hours in their branch due to fraud committed on the account after the account holder wrote a check to Chicago Title Company. The losses exceeded $2,600.

MORAL OF THE STORY

Operations who mishandle a customer's non-public information can suffer much more than just embarrassment. In some cases the costs are immeasurable. They face bad public relations with their customers, loss of business, the possibility of fines and loss of profit.

In this instance the customer was not satisfied with the offer of a free year's worth of CreditCheck® Basic through Experian®. As a result, the manager had to make a business decision which resulted in the loss of $2,600 to the operation.

If the escrow branch is sending copies of the earnest money check to un-entitled parties – meaning those individuals who should not otherwise have access to the buyer's non-public information – the MICR line of the check should be whited out or blacked out prior to sending the check copy.

That said, most lenders will insist the escrow holder provide a copy of the earnest money check unaltered. The lender already has access to the buyer's bank account information, since they had to supply the information to the lender in order to qualify for a new loan. The lender is entitled to the information.

The escrow holder complies with this request by sending an unaltered copy of the check and receipt using the Company's encryption software called Voltage. To find out more information on how to send an encrypted email, see escrow technical memorandum #148-2011, Secure Emails.

FRAUD Insights

DIVERTED funds

An independent escrow agent recently discovered their trust accounts were compromised by an outside unknown source. Through initial investigations the escrow agent realized they had become victim to unauthorized and fraudulent wire transfers. Once they became aware they immediately notified their bank, regulator and insurance carrier – as well as local and federal law enforcement.

The regulator – the Department of Corporations (DOC) – initiated an internal audit of the independent escrow agent. They discovered on three separate dates, funds totaling $1,558,339 were wired out of two separate trust accounts without authorization. The wires did not appear to be associated with any escrow processed by the company.

The DOC provided an opportunity for the independent escrow agent to cover the lost funds from their operating account, but ultimately concluded the escrow agent had lost so much money in the theft they could not cover the shortage.

The DOC froze the trust accounts to prevent further loss. The trust bank launched their own investigation and was successful in recovering a portion of the funds; lowering the shortage amount to approximately $1.1 million.

With their accounts frozen, the independent escrow agent had to notify all of its customers and principals in active transactions that they were unable to close any pending transactions.

The customers were notified they could transfer their transactions to other escrow companies, but they could not access the funds deposited with the agent. They went further to state in the notification, if any funds were to be transferred with the transaction it would have to be with the approval of the DOC who recently appointed a conservator.

The conservator must reconcile the total funds available with the potential claim to determine whether or not funds still on deposit can be released on a pro rata basis. The customers were notified they would not receive all of their funds.

The DOC website has been updated to include information regarding this incident under frequently asked questions (FAQs). Parts of the FAQs include notification that principals will have to replace any funds needed to close prior to the release of funds by the conservator, since the conservator will be performing a time intensive and extensive audit. The FAQs also revealed the freeze on the trust accounts resulted in checks returned by the bank when presented for payment.

MORAL OF THE STORY

Believe it or not our Company has fallen prey to this same sort of crime. We had to replace the stolen funds with money from our operating account. As a result, the Company is quickly deploying a Citrix® environment to those desktops belonging to personnel that have the authorization to initiate and approve outgoing wires using online banking. The Citrix environment eliminates the risk of the mime trick that first captures keystrokes and then delivers them to the hacker.

LAPTOPS and tablets

Laptop computers and tablets can serve as a great convenience but also carry a heavy responsibility as they are prime targets for theft. Here are some tips for preventing theft of the device or information contained on them:

- Do not leave a laptop or tablet unattended or unsecured in a public place including a hotel room, even for a moment. Use a locking cable to secure your system to a desk or other immovable object.
- Nearly 40% of all laptop or tablet thefts occur in offices. Be sure to secure your electronics in a locked cabinet or take them home with you.
- If your laptop or tablet contains a wireless device make sure it is turned off or disabled when not in use.
- Be sure to use the latest security measures by ensuring your laptop or tablet is password protected.

We use laptops and tablets for everything from online banking to storing important documentation. Be sure to take the proper steps to protect your device and your identity by ensuring you have antivirus software on your device.

Be wise about Wi-Fi in public wireless networks such as coffee shops, libraries, hotels and other public places. Before you use a public Wi-Fi network, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

SAFETY CORNER