OUR OFFICES WILL BE CLOSED ON DECEMBER 26th, 2016 AND JANUARY 2nd, 2017

Featured Program

Did you know?

You can now receive "LIVE" data from us to your "ToolBox" for your requested FARM data? Instead of receiving a "CSV" file that displays columns of information, you can now view the file on your computer with links to information such as:

- AERIAL VIEW MAPS
- STREET VIEW MAPS
- PROPERTY HISTORY
- ASSESSOR INFORMATION
- FORECLOSURE INFORMATION
- PROPERTY PROFILES, EXPORTABLE FARMS & SHAREABLE DATA
- EXPORTABLE DATA TO CSV, LABELS, 6 OR 12-LINE PDF FARM

Also, never again will you have to call to update your FARM(s) and your FARM(s) will now routinely updated such that the most recent property data is always available at your fingertips.

CONTACT US TODAY FOR MORE DETAILS!

December Fun Facts & Events

1. December Birthstone: Turquoise, Zircon, or Tanzanite
2. Zodiac Signs: Sagittarius (11/22-12/21), Capricorn (12/22-01/19)
3. December Flowers of the month: Narcissus
4. World's AIDS Day is celebrated on December 1st
5. December 3 - International Day of the Disabled Person
6. December is Universal Human Rights Month
7. December is National Read a New Book Month
8. In December, Nobel Prizes are awarded
8. December 13 is Poinsettia Day
9. December 25 is Christmas Day **(FEDERAL HOLIDAY IS 12/26/16)**
10. December 31 is Make Up Your Mind Day

ESCROW CORNER

FORGERY using an electronic signature

Marilyn Olliver, Division Manager of one of our Title agency, was covering the desk of a manager out on a much deserved vacation. One of the files she worked on was a sale where the buyer obtained a FHA insured loan. The seller was out of state and had already signed all of their closing documents, and provided written and signed Disbursement Authorization Instructions for the proceeds from the sale.

read more

ChicagoBlog is proudly brought to you by:

FORGERY using an electronic signature

The buyer's loan documents came in. The buyer signed off on the loan documents and left for the bank to initiate a wire of their closing funds. Since the loan was a FHA insured loan a few of the documents required the seller's signature. An assistant at the office emailed the loan documents to the seller to sign.

The seller emailed the assistant back stating she wanted to change the account where her proceeds would be wired. The body of the email included the new wiring instructions. The assistant replied with a blank copy of the Disbursement Authorization Instructions and asked the seller to complete them, then send them back with the other documents.

Marilyn was copied on the email. She noticed the account name for the new bank account was a company name and not the seller's name. Marilyn notified the seller the proceeds must be wired to an account in her name individually. Something about the email bothered Marilyn so she reviewed it closer.

Marilyn looked carefully at the email address comparing it to the one in the file and discovered the address was not the same. It was very close, but it was not the same. A fraudster was "spoofing" the seller's real email account. Marilyn picked up the phone and called the seller at a trusted phone number. She left her a voicemail and asked her to call regarding her closing so they could finalize everything.

While Marilyn waited for the seller to call back, the fraudster sent in revised wire instructions and continually asked for confirmation the wire was sent. The seller returned Marilyn's call and confirmed she had not sent revised instructions. Marilyn explained it appeared fraudsters hacked her email. The seller was very grateful North American Title Company caught this and thus protected her $246,000 in proceeds.

This story, however, did not end there because the fraudster did not let up. He again completed another Disbursement Authorization Instruction and signed it electronically in an attempt to divert the wire transfer. Furthermore, the fraudster electronically signed or forged the seller's signature on the loan documents Marilyn provided and returned them. The fraudster kept asking for confirmation the wire was sent.

Marilyn replied requesting the fraudster call her. The fraudster replied he was in meetings all day but she could always reach him by email. She replied she would not be able to send the wire until he called her. He did not respond.

Marilyn shared the emails with her corporate offices. Her corporate attorney then contacted the bank where the fraudster attempted to divert the proceeds. The attorney alerted them their account holder was up to no good. The bank's fraud department is investigating the account.

Marilyn sighed in relief. Thank goodness she took the time to trust her gut and review the email. She halted a large loss and a potential claim to the Company's errors and omissions insurance policy and saved the customer.

In hindsight Marilyn realized how difficult it was to detect forged documents signed electronically since comparing to live signatures she had was impossible. Marilyn said, "It is so important for everyone to be aware of all the fraud schemes out there today, and to pick up the phone and call your customers to insure that all instructions are correct instead of taking the easy route and emailing."

Although we have published many other articles in previous issues, this one features a new twist — the fraudster actually forging the seller's signature to other documents. Thank you Marilyn for sharing her story!

CHRISTMAS SCAM ALERT!

SAN FRANCISCO — As Christmas approaches, experts suggest an extra dollop of caution before clicking on email package delivery notices. Fake notifications are proliferating, bringing not holiday cheer — but holiday ransomware.

The holiday phishing season began just before Thanksgiving and will likely extend until after Christmas, said Caleb Barlow, vice president for IBM Security. Security company FireEye sees a significant increase in fake package email alerts beginning in November, an almost 100% increase from the average of September-October.

Common subject lines the company has been tracking include:

- We could not deliver your parcel, #00556030
- Please Confirm Your DHL Shipment
- Problems with item delivery, n.000834069
- Delivery Receipt | Confirm Awb no:XXX830169
- Your order is ready to be delivered
- Courier was unable to deliver the parcel, ID00990381
- Your DHL is here please download attachment to view detail and confirmation of your addresswas up to no good. The bank's fraud department is investigating the account.

It's important to remember legitimate shippers such as Amazon, FedEx and UPS have nothing to do with this and haven't done anything here.

To protect yourself, look carefully at any emailed package delivery notice. Do they include your full name, customer number and actual information from the company? Is the email address it came from actually the company or some odd variant? If there's any doubt don't click, experts say. Take the time to actually type in the Amazon or UPS or FedEx address. It won't take that much longer but will protect you.

SOURCE: USA Today.