# Wire Fraud Begins to Hammer the Construction Industry

Cybercriminals are adding new housing construction to their fraud landscape...and likely on a wide scale.

**Created and published by:**


### Thomas W. Cronkright II, Esq.

CEO/Co-Founder
CertifID LLC

1410 Plainfield Ave. NE
Grand Rapids, MI 49505

616.855.0855
www.certifid.com
tcronkright@certifid.com

### Lawrence Duthler, Esq.

President/Co-Founder
CertifID LLC

1410 Plainfield Ave. NE
Grand Rapids, MI 49505

616.855.7190
www.certifid.com
lduthler@certifid.com

# Wire fraud continues to grow within the housing and real estate industry at an alarming rate.

Experts estimated losses of $1B in 2017 alone. In real estate, wire fraud is the number one cybercrime in the United States. It's also continuously evolving in scope, complexity, and effectiveness. Each time the experts believe they have their heads wrapped around the "m.o." of the "typical" fraudster, a new scam is deployed and a new market segment is exploited. And now, unfortunately, housing construction is coming into the crosshairs.

## The size of the prize

In 2017, there were a reported 1,208,000 home starts in the U.S. Another estimated 1,266,000 will be started in 2018. The average sales price of a newly constructed home was $383,600, which amounts to $463B in total valuation of new inventory.**

The average time to build a home in 2017 was seven months. Most projects are structured so that monthly payments or "draws" are processed to pay for supplies and labor performed each month. That equates to 8,456,000 draws that may have occurred in 2017 with an average draw amount of $54,800. This represents a huge honeypot for cyber criminals to exploit – and they've already started.

In the past few months, we've assisted buyers in the recovery of funds sent to fraudsters after those buyers were deceived into thinking they were actually wiring funds to a trusted party in the transaction. Each time we peel back the layers of the fraud, we discover another important nuance in the algorithm used by fraud perpetrators to target new market segments and execute their frauds. To best demonstrate the sophistication and evolution of wire fraud as it targets the home builder today, here are three recent, "real-life" examples.

**All statistics reported courtesy of National Home Builders Association, via Western Michigan Home Builders Association.

# **CASE STUDY 1:** WIRING MONEY TO THE "BUILDER", NOT THE TITLE OR ESCROW COMPANY

Earlier this month, buyers in Grand Rapids, Michigan were preparing for a closing. As the final closing numbers were created, the buyers received an email from the builder requesting that they wire funds directly to the builder rather than the title company for closing. The amount was just over $150,000. The email from the builder and the wiring instructions that were attached included the builder's logo, name and title of the builder's representative that had been included in previous communications, and the correct amount they were expecting to send. The buyers, thinking the communication was coming from the builder, sent the wire. Days later they realized the builder had been spoofed (fraudulently imitated) and they had sent the money to a fraudster.

## How Did They Do It?

STEP 1 **Real Estate Agent Email Takeover.** It appears that the cybercriminals were able to penetrate the email account of the real estate agent representing the buyers. Once account access was obtained, they had the ability to monitor communications in real-time to identify a transaction to insert themselves into. They would have had access to the identity of the buyers, builder, lender and title company assisting in the transaction.

STEP 2 **Builder and Builder's Employee Spoofed.** Armed with the builder's information--right down to the level of the employee that was communicating with the buyers—the cybercriminals spoofed the identity of the builder by registering a domain name that was nearly identical to that of the builder. For example, if the domain name of the builder was www.zzzbuilders.com, the fraudster would register a domain such as www.zzzbuilder.com, leaving off the "s" in the actual domain name. Once the domain is registered, an email account was created and the email sequencing set to match that of the builder's employee, which was also spoofed. Taken a step further, the fraudsters made sure that the employee's name displayed the same way in the new email as it did in prior emails – after all, they had examples of such emails and knew exactly what to do.

STEP 3 **Fake Wiring Instructions Sent.** From the spoofed builder and employee email account, a convincing email was sent to the buyers requesting them to send their $150K payment to the builder, rather than the title company. The wiring instructions were attached to the email.

STEP 4 **Wire Sent to Fraudsters.** Thinking they were communicating with the builder, the buyers followed the instructions in the email and wired the funds to the fraudster. Monitoring their bank accounts in real-time, the fraudsters quickly followed up by moving the money between banks to avoid detection and thwart recovery.

Thankfully, the fraud was identified quickly. Authorities and experts assisted in identifying and "freezing" the funds from further transfer. However, these buyers are among the small percentage of "lucky" victims.

# **CASE STUDY 2:** HIJACKING MONTHLY DRAWS

In January, 2018, a lender finalized the paperwork necessary to fund a monthly draw to a builder. Just before the amount was to be wired, the bank received an email from the builder explaining that the builder had recently changed banks and, as a result, the draw would need to be sent to a new account. The lender, following its prescribed best practices, reached out to confirm the new information from the builder and the fraud was exposed. This was the first instance of that lender encountering a fraudster attempting to intercept a monthly draw disbursement. This lender, by the way, tended to be ahead of the curve (well ahead of the curve) in its fraud prevention techniques, which allowed it to thwart the fraud attempt. Many other lenders would have quickly fallen into the scam.

## How Did They Do It?

STEP 1 **Identify a Construction Project.** The cybercriminals monitor construction permit filings and identify active projects along with the builder name and contact information. Armed with this information, they target the builder, obtain access to its email account, and begin to monitor email traffic to identify a transaction to launch their fraud.

STEP 2 **"New" Bank Account Introduced.** From the builder's email account, a convincing email is sent to the lender explaining that the builder recently changed banking relationships and that the current draw and all further draws must be sent to the "new" bank. The wiring information for the "new" bank is included in the email. To make the email more credible, the fraudster mimics the language, tone and style of the builder…right down to the use of casual curse words and slang that the builder may have used in previous conversations with the lender.

STEP 3 **Monthly Draw Sent to Fraudster.** Having received the email directly from the builder's email account, the hope of the fraudster is that the lender would send the monthly disbursement without any further follow up or confirmation whether the communication actually came from the builder. This is a huge opportunity for fraud considering that the average monthly draw is likely to exceed $55k this year.

Thankfully, the use of this lender's best practices uncovered the fraud, stopping it in its tracks. However, the attempt highlights a scary reality – fraudsters are getting smarter and moving into other lucrative areas in real estate transactions.

# **CASE STUDY 3:** LOT PURCHASE "PAYOFF" SCAM

Many new construction projects involve the purchase of land from a developer prior to construction. The purchase may be made before the commencement of construction or after the construction is complete. Another cyber fraud includes the spoofing of the developer's identity and bank credentials so that funds used to purchase the land are diverted to the fraudster.

## How Did They Do It?

STEP 1 **Identity Spoofing.** The fraud starts by spoofing the identity of the developer or a developer's representative – typically an attorney assisting in the transaction. By gaining access to an email account of a party in the transaction, the cybercriminal obtains the information necessary to impersonate the developer or attorney. In some cases, the fraudster registers new domain names and creates email accounts that look convincingly similar to the company and employee they are impersonating.

STEP 2 **Payoff Letter Sent.** Knowing the exact timing of the closing and likely seeing the payoff request coming in from the title or escrow provider, the cybercriminal creates a payoff letter that includes all the information regarding the developer including the developer's name, address, contact information, payoff amount, per-diem interest and legal description, parcel number and, sometimes, even the address of the land being sold. We are beginning to see very convincing payoff statements designed to avoid any scrutiny on the part of the title or escrow provider.

STEP 3 **Create a Bank Account in the Name of the Developer.** In order to make the payoff more convincing and to avoid detection through automated bank account matching protocols, the fraudster opens a bank account in the name of the developer he or she is seeking to defraud. With very little effort, a company can be created, federal tax identification number issued, and corporate bank account established. With a bank account in the name of the developer, the fraudster significantly increases the chance of success by foiling best practices around bank account matching--all before funds are ever sent.

STEP 4 **Purchase Proceeds Wired to Fraudster.** Having received the payoff instructions and possibly confirming the name on the bank account, the title or escrow company unknowingly wires the funds to the fraudster.

The sophistication of this fraud is one of the most concerning as it exploits the trust of parties in the transaction and bank credentials. While current Know Your Customer (KYC) rules have improved the integrity of bank account openings, it has not prevented the ability for bad actors to open accounts for the purpose of defrauding third parties. There are simply too many variables to catch everything – especially at account opening.

# How to protect yourself and your client.

Lowering your risk profiles involves a commitment to training people, refining processes, and investing in technology that will identify and prevent attacks. The weakest link in the security chain is people, so start there. Educate all employees and transaction participants on the threat that fraud poses to everyone. Share phishing, spoofing and email account takeover examples and get aligned on how communications and wiring information will be exchanged.  Most importantly, make sure your customers are involved in this process. 2018 is not the year to take the position that fraud is "someone else's problem." Wire fraud is everyone's responsibility. As industry leaders and business owners, it's our role to guide our clients safely and securely through the process of building, buying or selling their homes.

CERTIFID

1410 PLAINFIELD AVE. NE, GRAND RAPIDS, MI 49505
PHONE NUMBER: (616) 855-0855
WWW.CERTIFID.COM
SUPPORT@CERTIFID.COM