State of New Jersey
DEPARTMENT OF BANKING AND INSURANCE
OFFICE OF THE COMMISSIONER
PO BOX 325
TRENTON, NJ 08625-0325
TEL (609) 292-7272

PHIL MURPHY
Governor

SHEILA OLIVER
Lt. Governor

MARLENE CARIDE
Acting Commissioner

BULLETIN NO. 18-04

TO: **ALL NEW JERSEY STATE CHARTERED BANKS, SAVINGS BANKS, SAVINGS AND LOAN ASSOCIATIONS, CREDIT UNIONS, NEW JERSEY LICENSED RESIDENTIAL MORTGAGE LENDERS AND BROKERS, MORTGAGE LOAN ORIGINATORS, TITLE INSURERS, TITLE PRODUCERS, AND LICENSED REAL ESTATE BROKERS AND SALESPERSONS**

FROM: **MARLENE CARIDE, ACTING COMMISSIONER**

RE: **WIRE TRANSFER FRAUD**

The industries addressed in this Bulletin handle millions of dollars in wire transfers every day in connection with mortgage loan transactions in this State. The purpose of this Bulletin is to remind you of the prevalence of fraudulent schemes to divert funds transferred by wire.

These scams generally involve several types of business email compromise ("BEC") techniques that alter normal wiring instructions to divert funds from the intended recipient to a stranger. BEC schemes may use social engineering or computer intrusion techniques, such as malware and phishing. With sophisticated hacking mechanisms, a perpetrator will target weakly guarded transactions and, for instance, send the buyer an email from an address nearly identical to the closing agent's, with a plausible subject line, advising of a "wiring change." When the buyer complies, the funds are wired to a scammer who is often overseas and usually impossible to track down. One precaution law enforcement agencies have urged is a "call and verify" routine, but scammers are now deploying phone "porting" technologies, to intrude into that safe-guarding process, masquerading as a trusted party.

There are innumerable versions of wire fraud, but they share one unfortunate result: the diverted funds are very difficult, if not impossible, to recover.

In these circumstances, this Department recommends that every regulated person that uses wire transfers be extremely careful when communicating wire transfer instructions electronically, and ensure that any third-party service providers are extremely careful. You should also take the time to inform all other legitimate parties to the transaction about applicable precautions.

To make your companies and your important transactions "harder targets," consider the following precautions:

- Closely verify email addresses before using them. Scammers mimic legitimate addresses and subject lines, but they are not 100% identical.
- Avoid web-based email.
- Strictly follow your specific business procedures for confirming the validity of changes made to wire transfer instructions.
- Use a confirmation process, which may include verbal communication via a mutually agreed telephone number between the known parties, as well as mutually agreed code words designed to combat phone "porting."
- Get to know the fraud resistance capacity of your third-party service providers, especially closing agents; become sufficiently aware of the relevant parties' normal wire transfer activity to recognize suspicious variations.

More information and guidance on these scams and their continually evolving nature can be found on the FBI's website, www.fbi.gov, and elsewhere by searching for "wire transfer fraud." If you believe your business is the victim of a BEC scam, you can file a complaint with the FBI's Internet Crime Complaint Center ("IC3"), at www.IC3.gov.

In New Jersey, you may also file an incident report with the New Jersey Cybersecurity & Communications Integration Cell ("NJCCIC"), at www.cyber.nj.gov, or with this Department, at http://www.state.nj.us/dobi/consumer.htm#banking. NJCCIC also offers a free membership to receive alerts, advisories, bulletins and training notifications.

4/10/18
Date

MCaride
Marlene Caride
Acting Commissioner