Let's Talk **Preventing Wire Transfer Fraud**

Financial Institutions have been targeted by criminals using wire transfer fraud schemes. These losses are preventable with appropriate policies and procedures, Owner training and awareness, and monitoring of accounts. Don't be a victim!

Why is wire transfer fraud so lucrative?

Cybercrime is attractive to fraudsters; potentially providing high returns with low risk. Because there is no personal contact with victims, enforcement agencies are hindered in the management of this growing fraud activity. This is a faceless crime and if the perpetrators are caught retribution is often minor.

Criminals are using a variety of methods to communicate and confirm wire transfer requests and succeeding. Often, Owners are unknowingly complicit in this fraud by responding to fraudulent communications either by phone or email and unwittingly providing their online banking access to unknown persons impersonating legitimate businesses believing they are protecting their privacy. Not so! Criminals are persuading people to run malware-laden attachments on their PCs, laptops, smartphones, tablets, etc. in order to gain access to personal email and the content of their email files which may have previously been exchanged with credit union personnel, potentially revealing account information and instructions for transferring funds.

Most people are not aware of the value of the information they possess and share through email communication and fail to protect that information.

How do they do that?

A typical wire transfer scheme originates with the compromise of an Owner's personal email account by a criminal. A subsequent email request is sent to the credit union asking for a wire transfer of funds, usually to a foreign country, and looks legitimate enough to unsuspecting credit union employees.

In fact the fraudster has taken over or "hijacked" the email account without the owner's knowledge. Follow up to the email request is dissuaded on the basis that the owner is not available for phone calls due to a business meeting, on vacation or other excuses.

Funds sent without the necessary assurances and safeguards in place are not recognized by the account owner until it is too late to recover.

Here's what Libro is doing to help protect your money:

- Our policies and procedures have been enhanced to ensure additional safeguards are in place for non-face-to-face requests for wire transfers received by telephone or email.
- Staff training for awareness of emerging fraud trends.
- Wire transfer requests received by email or phone are independently confirmed using contact information from the owner's file and NOT from the email or phone contact itself.
- Educating Owners on the safe use of their home and business communication devices.
- New security features ie: Two Step Verification.