First for Your Success

Wire Fraud

Train, Verify, Identify, & Report

Presented by: Cassie Orloske, *Data & Deposit Services Manager*
Joe Parish, *Senior Wires Support Specialist*

Panelists

Cassie Orloske
Data & Deposit
Services Manager

Joe Parish
Senior Wires
Support Specialist

2

Disclaimer

United Bankers' Bank (UBB) is providing this information as a service, it is neither a legal interpretation nor a statement of UBB policy. All statements contained herein are the sole opinion of the author. For any concerns which may arise, please consult your own internal policies and procedures.

3

What is a Wire Transfer?

A Wire Transfer is an irrevocable electronic transfer of funds.

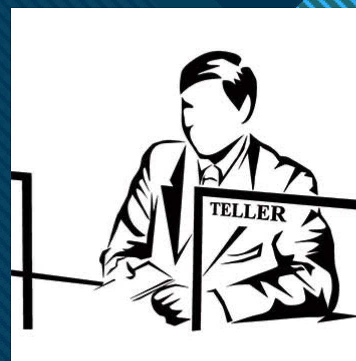
What does that mean?

It's essentially the same as handing cash over to someone. Have your Originators ask themselves the question – "Do I feel comfortable enough with this entity to hand them an envelope containing $10,000 cash?"

4

Mr. Jones' Wire

What would you do??



What is Wire Fraud?

Financial fraud involving the use of telecommunications or information technology

Some Common Wire Fraud Schemes:

- Advance Fee
- Catfishing/Romance Scams
- Business Email compromise fraud
- Phishing
- Telemarketing

Preventative Measures

To understand how consumers are protected, let us take a look at three major electronic payments systems used in America and what's in place to prevent fraud from occurring

7

Preventative Measures

DEBIT/CREDIT

- MC/Visa Mandates
- Regulations
- Spending limits
- EMV/Contactless technology
- Behavioral anomaly detection software
- Authorization filters

ACH

- NACHA Rules and Regulations
- Authorizations
- Origination limits
- Originator observation
- Behavioral anomaly detection software
- Unauthorized return limits

WIRE TRANSFER

- US

8

Wait?!
What do you mean “Us”?

Financial Service Professionals: the Front Line to Prevent Wire Fraud

We are the Front Line to Prevent Wire Fraud

- We have a responsibility to do all we can to prevent fraudulent transactions from taking place:
  - Train
  - Verify
  - Identify
  - Report

Ensure Frontline Staff Training

Our employees are our greatest asset and first line of defense against wire fraud!

11

Ensure Frontline Staff Training

- Make sure staff are up to date on all required trainings, which may include:
  - Customer Identification Program
  - Deposit Operations: BSA and AML Considerations
  - Suspicions Activity Reporting
- Encourage Staff to take additional trainings:
  - Detecting and Preventing Wire Fraud
  - Identifying Types of Wire Fraud
  - State or National Banking Associations

12

Verifying Customer Identity

Ensure our customers are who they say they are!

Verify Customer Identity

- As fraudsters get more sophisticated, banks must adapt their approach in how they verify client identity. We cannot solely rely DOB's, last four of socials, or even account history because this information may have already been compromised.

Verify Customer Identity

What are some additional ways to authenticate a caller?

- At which branch did you open your account?
- Who did you open your account with?
- Who is the joint owner on your account?
- What is your safe deposit box number?
- Who is the POD on your account?
- These questions can also work in reverse, such as asking who the joint owner is on a single account.
- After authenticating a caller or upon an in person visit, you may set up an account password to use in lieu of verification questions.

15

Verify Customer Identity

The Power of a "Call Back"

- When in doubt you can always call back using the phone number you have on file for your account holder.
- In many cases, a call back verification is standard procedure at many banks when initiating a wire transfer through email or phone. We must be cautious when updating contact information.

16

Verify Customer Identity

The Power of a "Call Back"

- When initiating a wire and conducting a call back, check to see if the phone number has recently been updated.
- For business clients, you may be able to authenticate a phone number from what is published on their website.
- Fraud can happen from an internal email intrusion as well. Call back for a wire requested from another bank employee via email or phone is also advisable.

17

Identifying Red Flags

Getting some information from your customer regarding a wire can help catch suspicious activity

18

Identify Red Flags

- Asking the:
  - Who
  - What
  - When
  - Where
  - Why

  …while initiating a wire transfer can uncover unusual behavior, if someone may be taken advantage of or sending funds under other false pretenses.

19

Identify Red Flags

- Identifying red flags can often help prevent a fraudulent wire from being sent in the first place.
- Once sent, a wire transfer is very difficult to get back, especially when the beneficiary bank is located in a foreign country.
- Remember, if you suspect a wire may be fraudulent, you can always **refuse to send** it.

20

Identify Red Flags

- **How can I refuse to send a wire? Isn't the customer always right?**
  - The customer isn't the wire or financial services expert, you are!
  - You can listen and hear what the customer is saying with an empathic attitude.
  - You are ultimately responsible to protect the customer AND protect your bank from potential financial losses.

21

Identify Red Flags

What questions should I ask?

- Relationship details
  - Who is the beneficiary? Relative, friend, stranger?
  - When was contact first initiated? Was contact made via email/ text messages/ social media? Who initiated contact?
  - What happened between then and now?
- Explanation of payment
  - Why is the payment being sent, what is the payment for?
  - Where did the wiring instructions come from? If emailed, was verbal verification completed? Do the wiring instructions look like they're from a legitimate source? Are they on company letterhead?
- Account Activity
  - What were the source of funds? Was there a recent check deposit to the originators account? If so, who was the check from? Are the funds collected?
  - Has this customer ever sent a wire before?
  - Is this a foreign wire? Is the beneficiary an individual?

22

Identify Red Flags

- Examples of Red Flag Scenarios
  - Foreign wires on a consumer account
  - First wire for your account holder
  - Receiving and/or sending wires on a new account
  - An urgent wire
  - Wire for tech support/Computer has a virus
  - A change in wiring instructions, especially changed via email
    - Look for changes in the email address and poor grammar

23

Identify Red Flags

- Examples of Red Flag Scenarios
  - Wire for money deposited to account my mistake
    - Overpayment
    - Look for recent transfers
    - Customer may see deposit, but not realize it’s from their other account.
  - Wiring funds from a mobile deposit
  - Moving funds across payment rails
    - Wiring funds out from an ACH deposit
    - Could be followed by ACH dispute

24

Identify Red Flags

- **Examples of Red Flag Scenarios**
  - **Bail relative or friend out of jail**
  - **Customer's account compromised/needs to wire money out in order to protect it**
  - **Wire for a retail transaction that processed as a credit vs. debit**
  - **Wiring funds related to social security number or other criminal offenses in order to stay out of jail**
    - **Any one claiming to be a law enforcement officer instructing customer to wire money**
  - **Sending funds that are going to "come back"**
  - **Customer not wanting to disclose the purpose of a wire.**

Identify Red Flags

The Value of Developing Customer Relationships

- When we are truly invested in getting to know and develop relationships with our customers, we can leverage that relationship partnered with our knowledge to help the customer identify requests that are unusual or suspicious!

Identify Red Flags

The Value of Developing Customer Relationships

- At a previous bank position, one of our UBB teammates developed a great business relationship with a customer that was building a new home in another country.
  - "My client came into the bank frequently to wire money to vendors for different building supplies. One day they came in and said they had been instructed to send a wire as soon as possible to a bank in a country they hadn't wired to before. They told me if I didn't send the wire right away it would delay their project. Knowing the previous payment patterns, I questioned the urgency and the new recipient. Upon further reflection the customer waited to send the wire and came back a few days letter letting me know it was a scam!"

27

Reporting Suspicious Activity

My Account Holder is Reporting Wire Fraud, Now What?

28

Reporting Suspicious Activity

Even with the best preventative measures in place, fraud can still happen.

- How to help your customers after fraud occurs
- What to expect from a fraud investigation

29

Reporting Suspicious Activity

In order to prepare for what may be requested by the receiving financial institution, we typically like to gather some details and documentation regarding the fraudulent activity

- A copy of your internal wire transfer request form and supporting documents
- Timeline of events including Correspondence between originator and beneficiary
- Nature of the fraudulent transaction
- Payment details including original wiring instructions
- Law enforcement documents

30

Reporting Suspicious Activity

- When reporting a fraudulent wire, time is of the essence. The quicker we can get word to the receiving bank that fraud has occurred, the better.
  - It is also advised that:
    - your account holder files a police report with the local authorities
    - your bank files a Suspicious Activity Report with FinCEN

31

Reporting Suspicious Activity

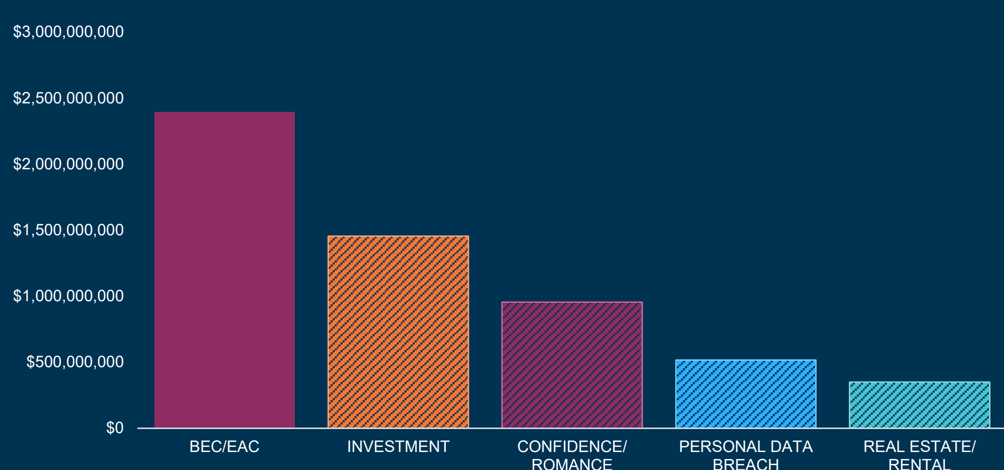
- Unfortunately, with Wire Fraud there is no guarantee that funds will come back to the originator's account.
- Resolution time can vary from bank to bank and the amount of fraudulent activity to the beneficiary's account is also a factor.
- If there are multiple victims and limited funds, it helps our case to respond quickly with any documentation requests made by the receiving bank. Recovery is usually first come, first serve.

32

Reporting Suspicious Activity

- If our recovery efforts are successful, we may expect funds returned within about a 90 day timeframe.
- If there is no recovery, at minimum we have alerted the receiving bank and authorities of what occurred to help prevent future fraudulent transactions.
- United Bankers' Bank is committed in assisting you in every way possible.

2021 Top Crime Types by Loss



*BEC = Business Email Compromise
*EAC = Email Account Compromise
*Data from the 2021 FBI Internet Crime Report

Q & A

Presented by: Cassie Orloske, *Operations Support Supervisor*
Joe Parish, *Senior Wires Support Specialist*

35

Thank You!

UBB *First for Your Success*

More questions? Reach out to Cassie at cassie.orloske@ubb.com or Joe at joe.parish@ubb.com