# Business Security Threats

FIRST FINANCIAL BANK

Presented by:

# What is Cyber Crime ?

**U.S. Department of Justice divides computer crime into three categories:**

1. Victim of Stolen Property (i.e. user ids, passwords, software, propriety data, confidential data, misdirected payments)

2. Victim of disruption or destruction of property that causes damage (i.e. files deleted, DDOS attacks, ransomware)

3. Victim of system takeover to commit crime (i.e. botnets, money laundering, distribution of child pornography, bank account takeover)

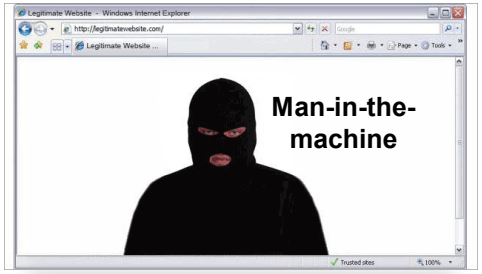
# Cyber Attacks

## How can my business be attacked?

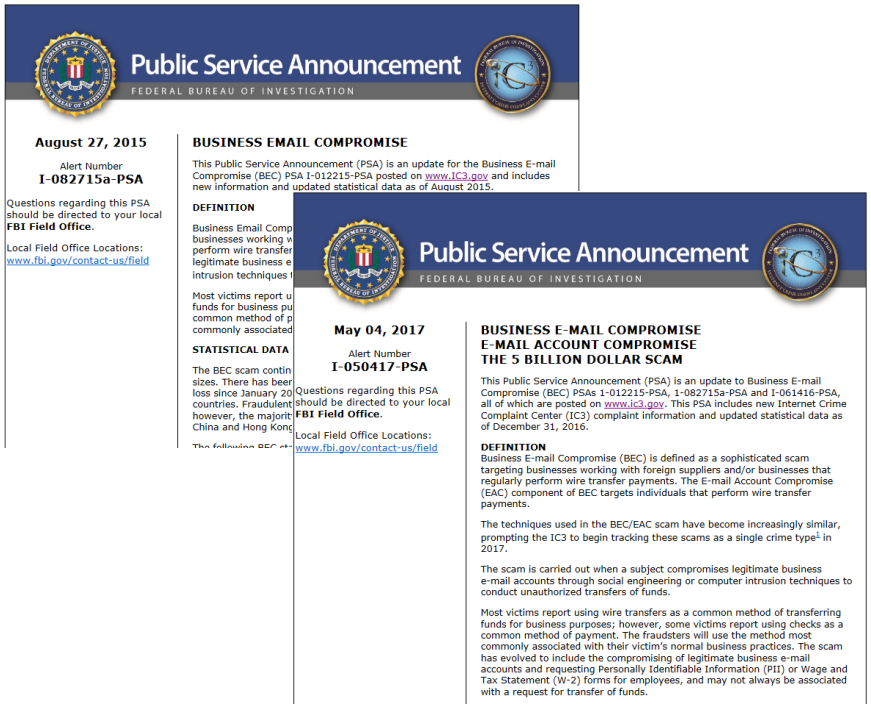
- Email links that direct you to fake websites requesting information
- Legitimate websites are hacked or malware inserted on page
- Unsecure Wireless network used without further protection
- Software is out-of-date with vulnerabilities just waiting to be abused
- Email compromise
- Improper operational controls

# Knowledge is Protection

- **Spoofing** – fraudulent email where someone is masquerading as a legitimate person in order to falsify data and get the receiver to initiate a transaction.
- **Phishing** – fake email messages that look real; ask for credentials and redirect to a counterfeit website.
- **Vishing** – fake phone calls pretending to be an authorized user; asking for information and credentials.
- **Malware** – keyloggers, account hijacking, "man-in the-browser", etc.
- **Pharming** – installs malicious code on your PC without conscious action.
- **"Man-in-the-middle"** – where networks are exposed to the public and data is intercepted, compromised or manipulated.
- **Social Engineering** – gathering of one's personal information through a variety of channels to be later exploited.



# Hot Topics



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

August 27, 2015

Alert Number
I-082715a-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

**BUSINESS EMAIL COMPROMISE**

This Public Service Announcement (PSA) is an update for the Business E-mail Compromise (BEC) PSA I-012215-PSA posted on www.IC3.gov and includes new information and updated statistical data as of August 2015.

**DEFINITION**

Business Email Comp
businesses working w
perform wire transfer
legitimate business e
intrusion techniques

Most victims report u
funds for business pu
common method of p
commonly associated

**STATISTICAL DATA**

The BEC scam contin
sizes. There has beer
loss since January 20
countries. Fraudulent
however, the majorit
China and Hong Kong

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

**BUSINESS E-MAIL COMPROMISE**
**E-MAIL ACCOUNT COMPROMISE**
**THE 5 BILLION DOLLAR SCAM**

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

**DEFINITION**

Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type[1] in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

- Business Email Compromise
- Ransomware
- Tech Support Fraud
- Elder Fraud

# Business Email Compromise (BEC)

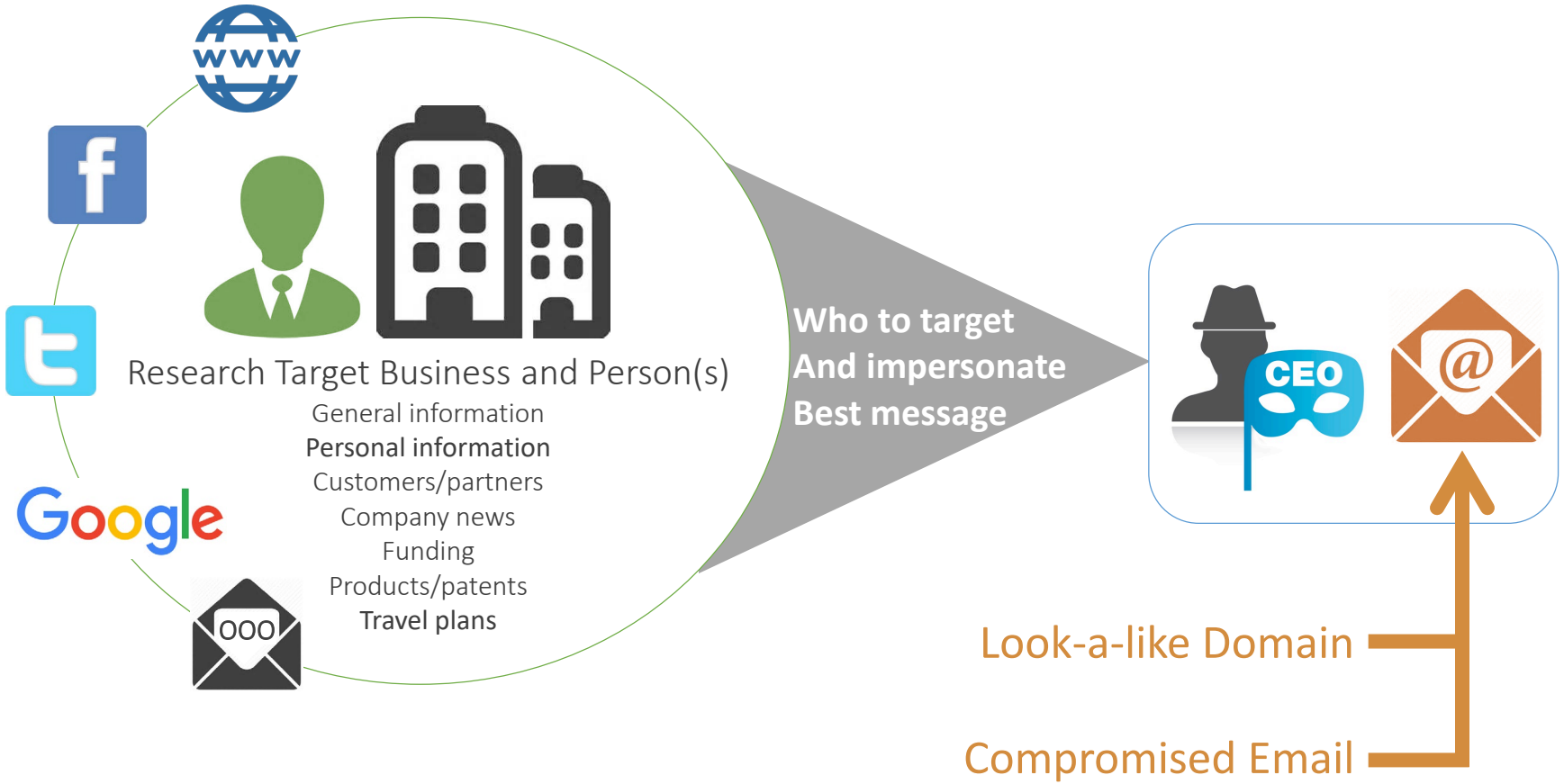
## Three Examples of BEC Attacks

Simple wire request from compromised email account

Fake Vendor Invoice

Elaborate story designed to make it believable

# How do the fraudsters decide who to attack?



# How it happens…

Create look-a-like domain

e.g. …@payrne.com vs. …@payme.com

(can you see the difference?)

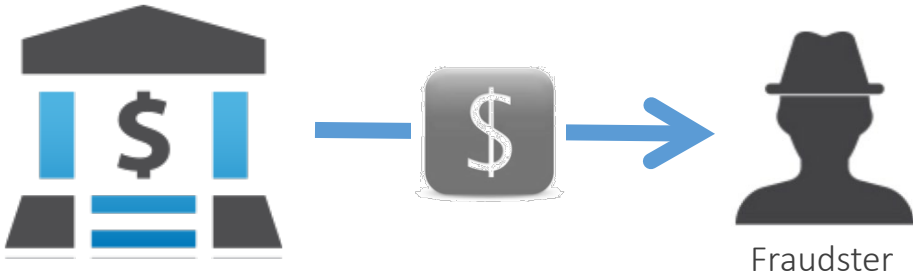
Fraudster sends email posing as CEO

Controller

Submits wire request

Confirmation

Approval



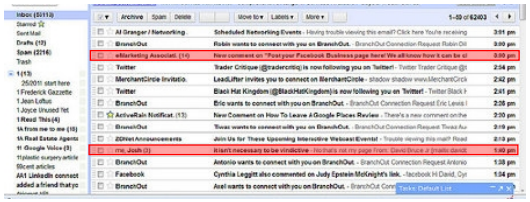

Fraudster

# How it happens…

"Please wire funds into an alternate account."

Finance Dept.

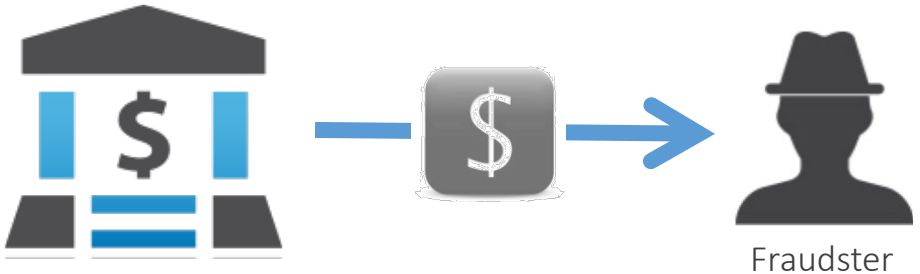
Search compromised email for vendor invoices



Wire request

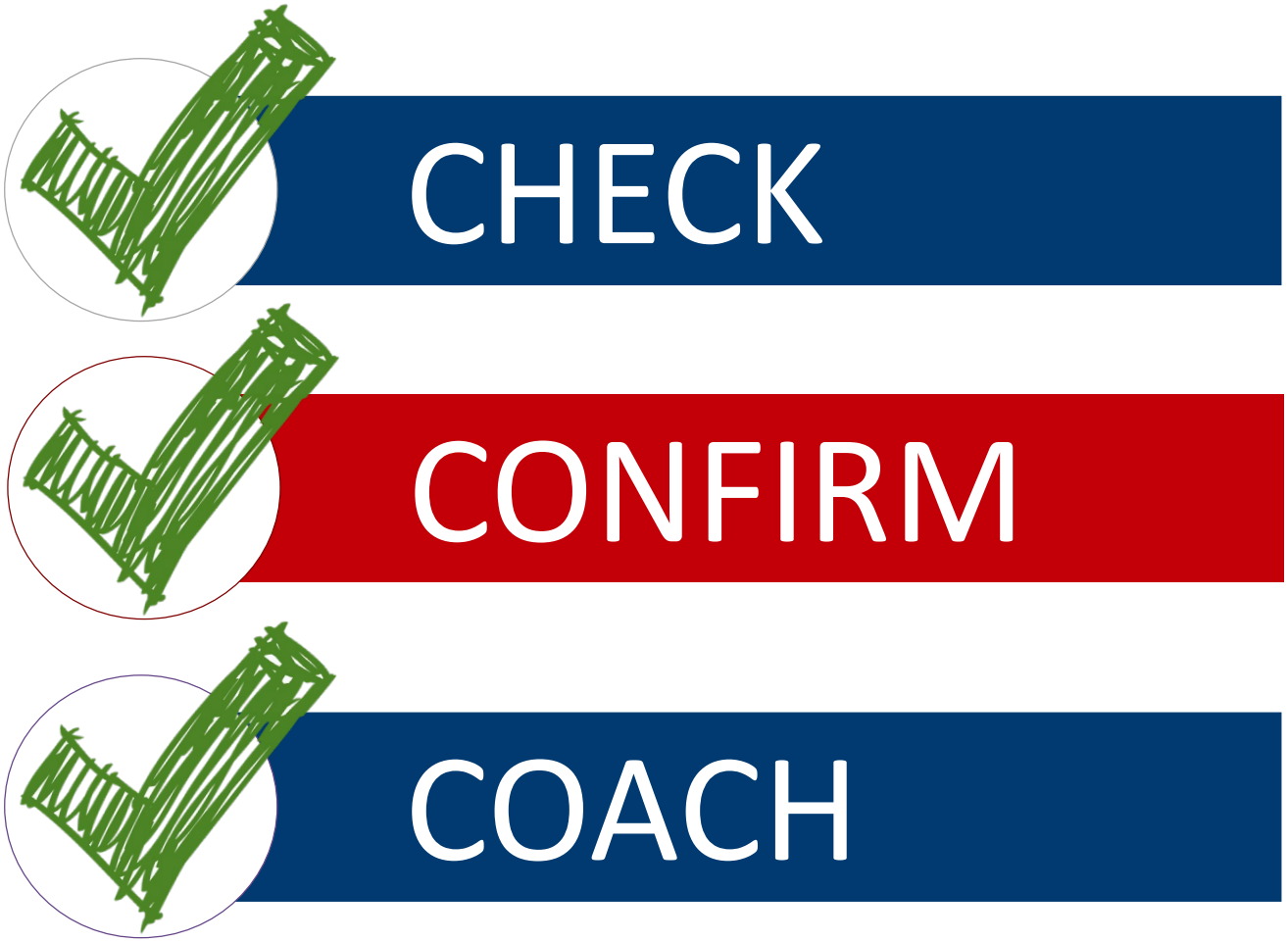
Confirmation

Approval

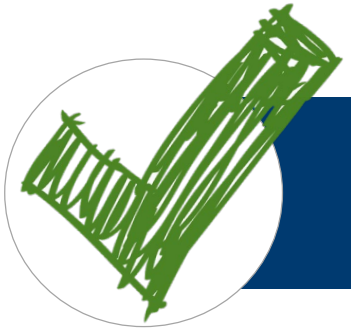


Fraudster

# Best Practices for Detecting BEC Fraud



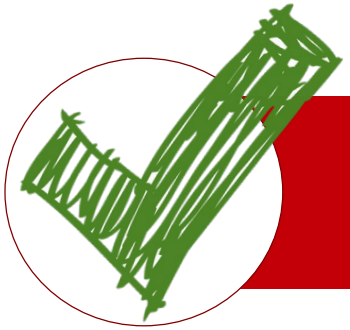
# Best Practices for Detecting BEC Fraud



## CHECK

- ✓Check for correct email addresses
  - ✓…@.co vs. …@.com
  - ✓…@greatsuccesss.com vs. …@greatsuccess.com
  - ✓…@abc-company vs. …@abc_company.com
- ✓Check for requests for secrecy or urgency
  - ✓Be suspicious of “only use Reply” or “only call me at this number”
- ✓Check for consistency with earlier wire payments
  - ✓Does the CEO typically request wire payments via email?
  - ✓Check prior vendor invoices for domain, timing, frequency, beneficiary, …

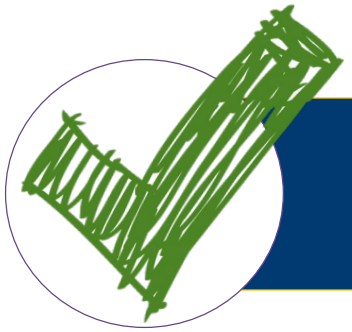
# Best Practices for Detecting BEC Fraud



## CONFIRM

- ✓Use an alternate communications channel to confirm the request
- ✓Ask the CEO!
  - ✓ Which would be worse: reconfirming the request or having money stolen?
- ✓Implement dual controls

# Best Practices for Detecting BEC Fraud

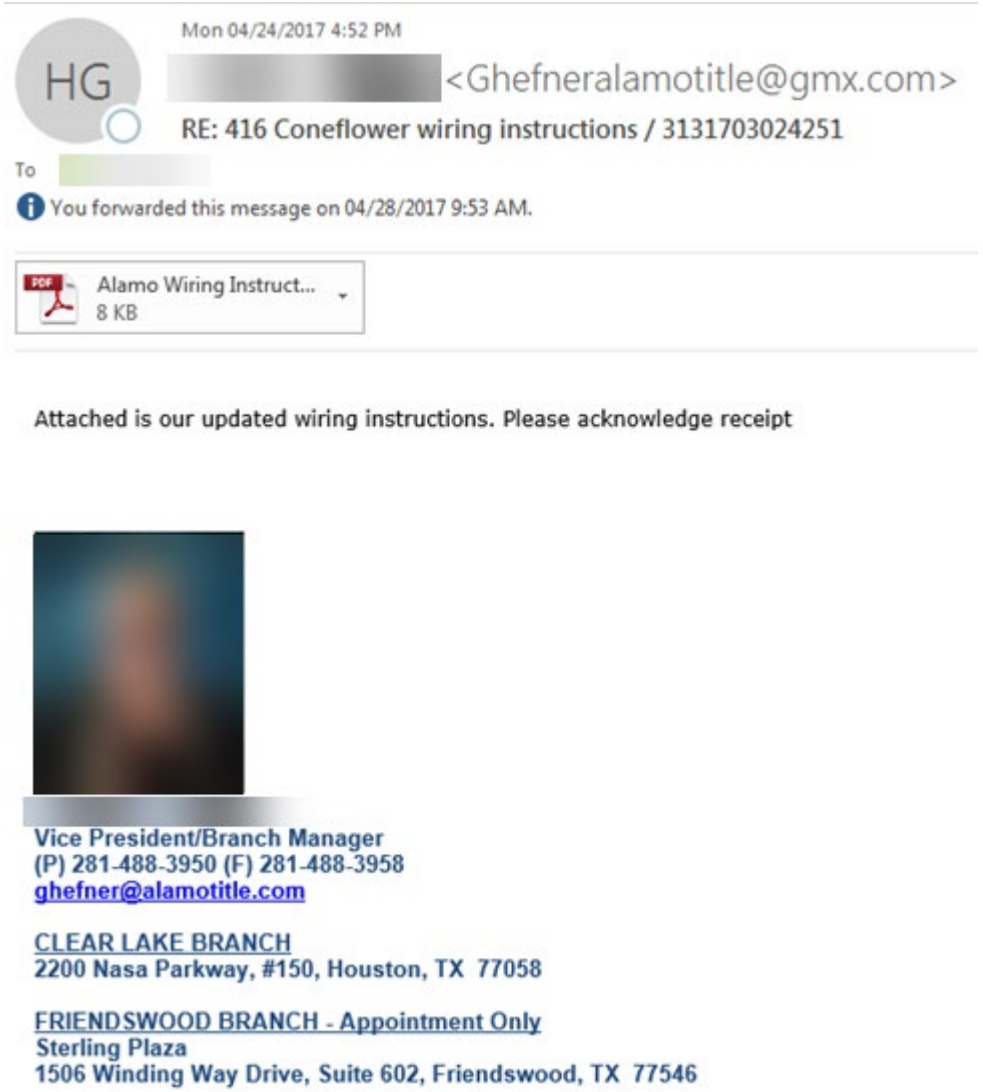


## COACH

- ✓Coach your employees
- ✓Coach your executives to encourage and support employees double checking wire requests
- ✓Be conscious of how information on website and social media can be used
- ✓Trust your financial institution

# BEC Example: Wire Fraud

Email Received by our Mortgage Officer



Mon 04/24/2017 4:52 PM

HG [redacted] <Ghefneralamotitle@gmx.com>

RE: 416 Coneflower wiring instructions / 3131703024251

To [redacted]

You forwarded this message on 04/28/2017 9:53 AM.

Alamo Wiring Instruct...
8 KB

Attached is our updated wiring instructions. Please acknowledge receipt

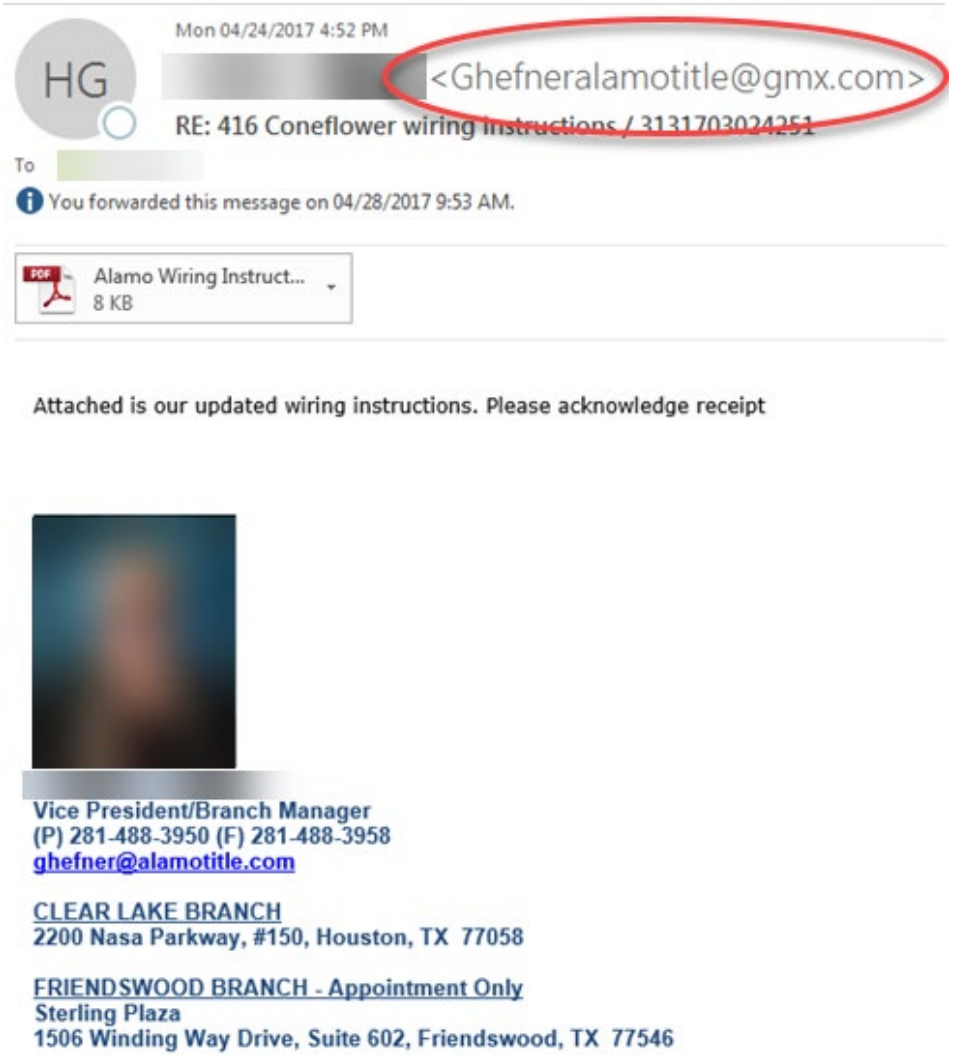
[redacted]

Vice President/Branch Manager
(P) 281-488-3950 (F) 281-488-3958
ghefner@alamotitle.com

CLEAR LAKE BRANCH
2200 Nasa Parkway, #150, Houston, TX 77058

FRIENDSWOOD BRANCH - Appointment Only
Sterling Plaza
1506 Winding Way Drive, Suite 602, Friendswood, TX 77546

# Email Received by our Mortgage Officer



Mon 04/24/2017 4:52 PM

HG [redacted] <Ghefneralamotitle@gmx.com>

RE: 416 Coneflower wiring instructions / 3131703024251

To [redacted]

You forwarded this message on 04/28/2017 9:53 AM.

Alamo Wiring Instruct...
8 KB

Attached is our updated wiring instructions. Please acknowledge receipt

[redacted]

Vice President/Branch Manager
(P) 281-488-3950 (F) 281-488-3958
ghefner@alamotitle.com

CLEAR LAKE BRANCH
2200 Nasa Parkway, #150, Houston, TX 77058

FRIENDSWOOD BRANCH - Appointment Only
Sterling Plaza
1506 Winding Way Drive, Suite 602, Friendswood, TX 77546

# Wiring Instructions

Alamo Title Company
2200 NASA Parkway, Suite 150
Houston, TX 77058
Phone (281)488-3950 * Fax (281)488-3958

Date: April 11, 2017
GF#: ATCH17068092
Property Address: 416 Coneflower Rd, League City, TX 77573

## WIRING INSTRUCTIONS

REFERENCE: GF#: ATCH17068092
Name:
Attn:

WIRE TO: KEY BANK
127 Public Square
Cleveland, OH 44114
ABA#: 041001039

CREDIT TO: Alamo Title Company
Escrow Account
Acct. #: 126122043931

PLEASE BE ADVISED THAT WE WILL ACCEPT ONLY WIRE TRANSFERS. WE CANNOT ACCEPT ACH DEPOSITS, PHONE FUNDS TRANSFERS OR OTHER TYPES OF ELECTRONIC PAYMENTS/CREDITS. THESE INSTRUCTIONS ARE FOR THE PURPOSE OF SENDING WIRE TRANSFERS ONLY.

Explanation: ACHS are typically created via online banking. While your bank may indicate you are sending a "wire" if you are initiating this "wire" online, you are in fact creating an ACH. Please contact your Bank for their wire process. NO ACHS, Electronic Payments/Credits or phone funds transfers will be accepted, and sending any funds via ACH, Electronic Payment/Credits or phone funds transfers will result in a delay in funding.

These are the Wiring Instructions for this transaction, they will not change. In an effort to increase security, should you receive any request to change these instructions, please call Glennie Hefner (Closer) at (281)488-3950.

# Scams for Finding Mules

## Nice to Know You

**Naomi Surugaba [azlin@moa.gov.my]** Actions

*Inbox* Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

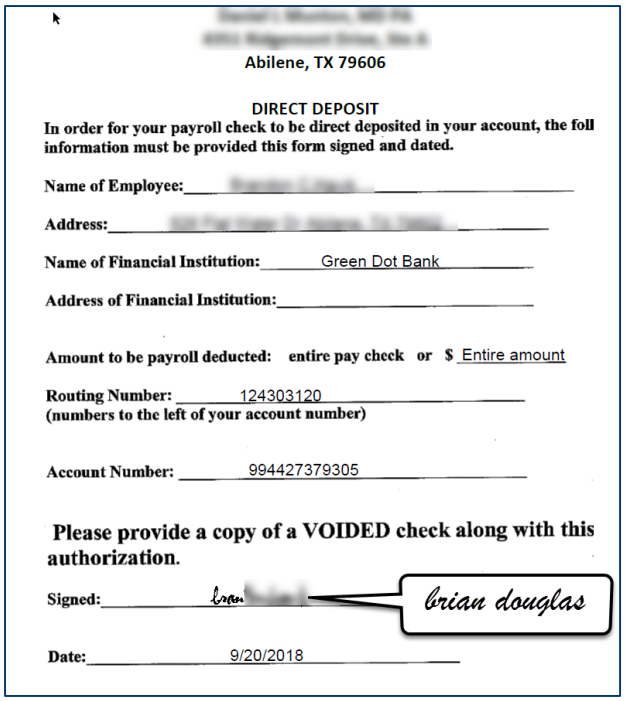
# Employee Payroll Misdirected

## It started with an email to the Office Manager:

**From:** [redacted]
**Sent:** Thursday, September 20, 2018 9:07 AM
**To:** [redacted]
**Subject:** direct deposit adjustment

Please I want to make a change to my direct deposit,I would like my next paycheck going to my account already on file to be sent to a new account that i will be providing,do i need to fill a form or just send void check copy of mine?

## The Office Manager sent the forms back via email reply and received this in return:



[redacted]
Abilene, TX 79606

**DIRECT DEPOSIT**
**In order for your payroll check to be direct deposited in your account, the foll information must be provided this form signed and dated.**

**Name of Employee:** [redacted]

**Address:** [redacted]

**Name of Financial Institution:** Green Dot Bank

**Address of Financial Institution:** _____

**Amount to be payroll deducted:** **entire pay check** **or** **$** Entire amount

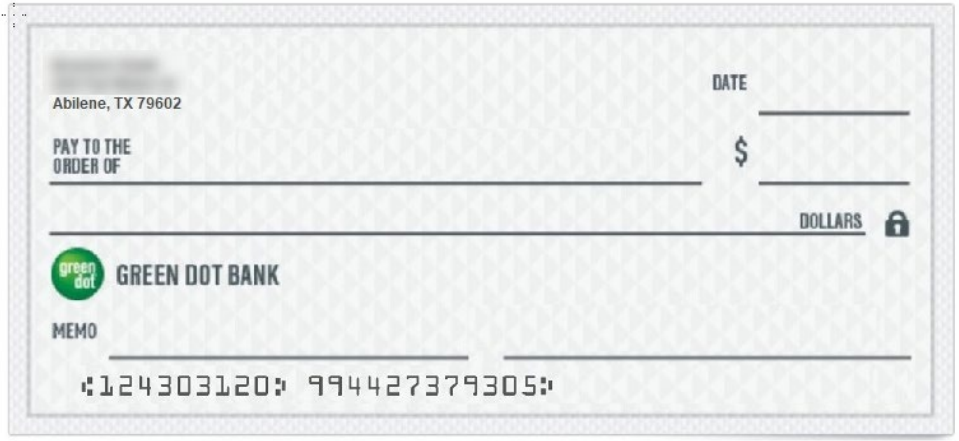
**Routing Number:** 124303120
**(numbers to the left of your account number)**

**Account Number:** 994427379305

**Please provide a copy of a VOIDED check along with this authorization.**

**Signed:** [redacted] *brian douglas*

**Date:** 9/20/2018



[redacted]
Abilene, TX 79602

DATE _____

PAY TO THE ORDER OF _____ $ _____

_____ DOLLARS

GREEN DOT BANK

MEMO _____

⑆124303120⑆ 994427379305⑆

Four payrolls later the employee realized his pay had yet to be deposited into his account.

# Protect Your Business – take away

# Protect Your Business

## It starts here – Basic Steps Include:

- Employ a security provider to install commercial anti-virus, desktop firewall and anti-spy software on all computers. Keep up-to-date.
- Update your security software; download & install security patches to operating systems & browsers as soon as they are available.
- Adjust browser settings to prompt your users whenever a web-site tries to install a new program.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Never access bank accounts at wireless internet cafés, or from public Wi-Fi hotspots, such as libraries, hotels & airports.
- Be suspicious of e-mail purporting to be from a financial institution, government department or other agency that requests account information, account verification, or banking access credentials.

# Protect Your Business

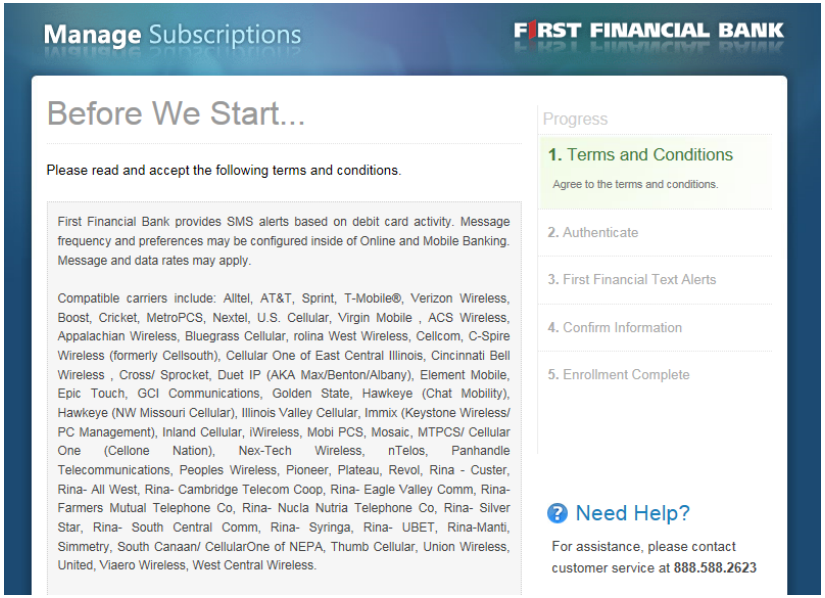
## It starts here – Basic Steps Include:

- Look out for changes in websites; Is the site asking you for more information than normal?
- Avoid opening file attachments or clicking on web links in suspicious emails.
- Create a strong password with at least 8 characters. Mixed case letters, numbers & special characters.
- Use a different password for each website that is accessed. Change your password a few times each year.
- Prohibit the use of “shared” usernames and passwords for online banking systems.
- Business & personal bank account usernames & passwords are different.
- Don’t use the same names & passwords for e-mail & social networks.
- Make a conscious decision on which computer should be used for general web browsing & social networking. Create a policy or system controls.
- EDUCATE YOUR EMPLOYEES!

# Debit Card Text Alerts

## Best Way to Protect Yourself

**Sign up for debit card alerts** to receive a text message anytime your card is used at ffin.com/alert



FIRST FINANCIAL BANK

# Do Not Become a Victim of the Most Common Scams

At First Financial, we want you to protect yourself against fraud. Here are some tips on how to protect yourself common scams.

*Internet Merchandise Scams*
If a website is offering an item at hundreds of dollars cheaper than retail (think: high-end sneakers), chances are that there's something fishy going on. Check out the reviews of the website and try calling the customer service line (if one exists).

*Prizes, Sweepstakes, and Free Gifts*
If you are asked to pay money – whether via wire transfer, gift card, prepaid debit card, or some other means – before you can receive your "prize," then it's a scam. Run away!

*Fake Check Scams*
If someone asks you to deposit a check into your personal checking account and then send all or a portion of the proceeds to them or someone they know, it's a scam.

*Recovery/Refund Scams*
These scams target people who have already lost money to another fraud. The scammer claims to be able to recover your lost funds for a fee. Don't wire them money, give them credit or debit card details, send a check, or give them any personal information. Just hang up the phone or delete that email!

*Advance Fee Loans/Credit Arrangers*
Consumers looking for a loan may be tempted by flashy ads on social media or the Web offering easy cash without a credit check. Be afraid! Any legitimate lender is going to want to at least check your credit history before offering a loan. Be especially wary if you are asked to pay a big upfront fee to get the "loan."

*Phishing/Spoofing*
Fraudsters are highly effective at making their emails and robocalls look and sound convincing. Beware of clicking on links or attachments in an email that seems to be coming from a bank or other trusted institution. Instead, type in the bank's web address or call the number on the back of your bill to verify before giving out any sensitive information like your bank account routing number, usernames or passwords.

*Friendship and Sweetheart Swindles*
If someone you met online suddenly wants you to send money to pay for a family emergency or for them to come visit you, it's probably a trap. Romance scammers will strike up relationships with dozens or hundreds of victims in the hope of convincing them to send cash. Be especially wary if your new friend quickly asks you to move the conversation to text message, chat apps, or email instead of a dating website's messaging platform.

*Computer Equipment/Software*
This is the dreaded "tech support" scam. If someone calls or emails you claiming to be "tech support" for Microsoft, Google, Best Buy, or some other technology firm, hang up the phone or delete the email. Chances are, they just want you to grant access to your computer so that they can convince you to pay for an expensive "tech support" service you don't actually need. Even worse, they can install malware or even encrypt your files and hold your computer for ransom.

*Scholarships and Grant Scams*
Fraudsters offering "guaranteed" scholarships or college grants are to be avoided. Chances are, they're just looking for a big fee in order to send you information about financial aid that the government already offers for free.

*Family/Friend Imposter*
An urgent call or email from a family member asking for help can be hard to resist. The call or email may also come from someone saying they're a lawyer, a doctor, or a law enforcement official that is in contact with your loved one. The "emergency" requires you to send money urgently. Before sending the money, try contacting the person in question or their parents on your own to verify the story first. Chances are, it's a scammer trying to get you to send money before you can stop and think.


© 2019 First Financial Bank,
Member FDIC | ffin.com

# Questions?

Scott Dueser, Chairman, President, CEO
First Financial Bank
400 Pine
Abilene, TX 79601
sdueser@ffin.com
(325) 627-7031