

# 2023 WIRE TRANSFER FRAUD UPDATE & BEST PRACTICES

Tony Taylor, CISO



5/22/2023

# Agenda

- ☐ Threat Landscape

- ☐ Anatomy & Type of Attacks

- ☐ Tips and suggestions to avoid becoming a victim

- ☐ Wire Transfer 'Best Practices'



# THREAT LANDSCAPE

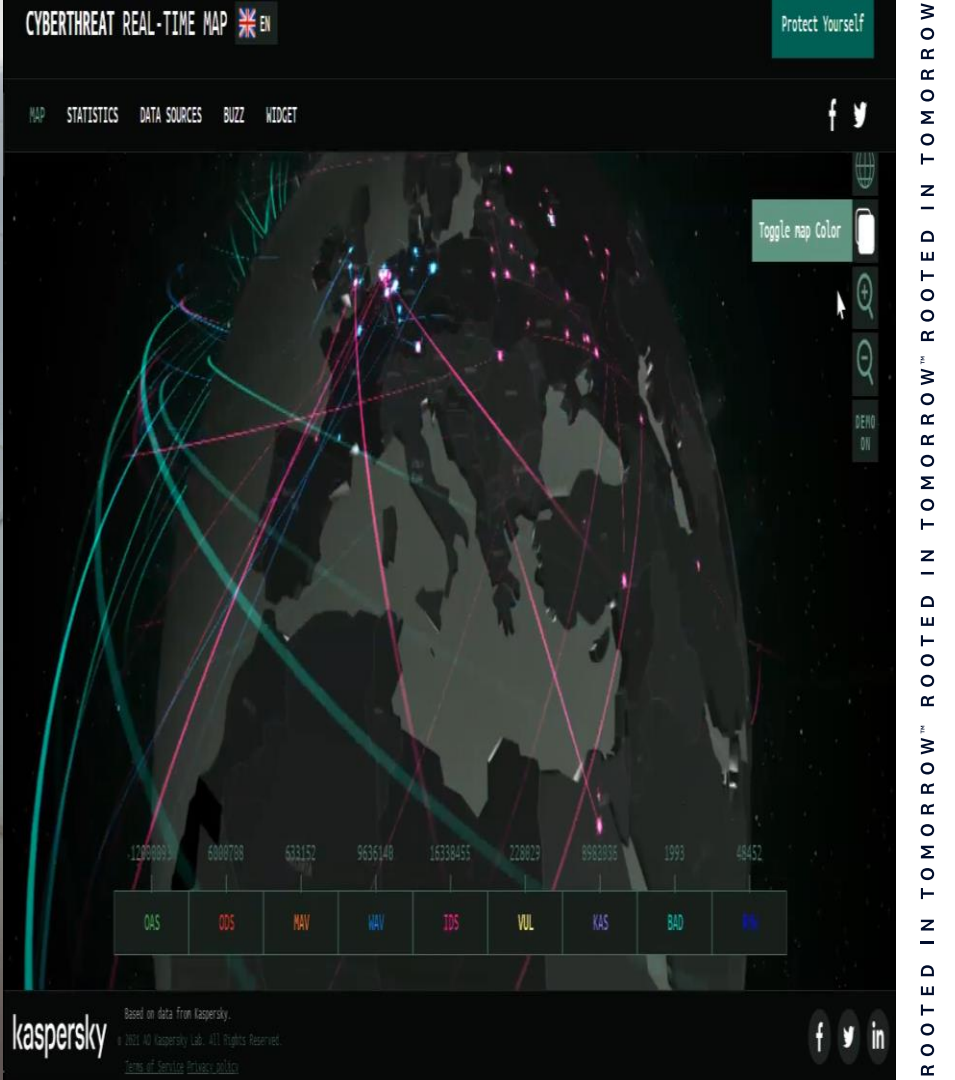
**Ransomware - Cyber Weapon of Choice** – Tremendous growth and threat actor's new favorite tool of choice

**Expanding attack surface** – Remote Worker, IoT, Supply Chain & Cloud adoption create new avenues for threat actors to penetrate

**Social Engineering** – majority of breaches still 'begin' with a phishing exercise that allows threat actors access to organizations internal networks

**Supply Chain** – Third parties sustaining breaches impacting upstream business operations

**Cloud Adoption** – new skills required to securely manage

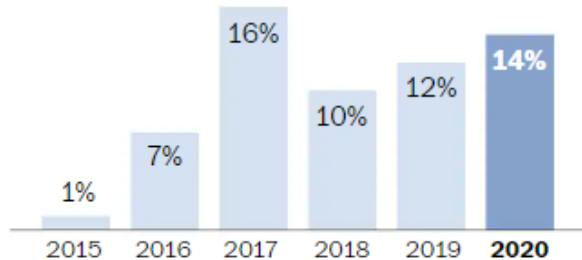


# Significant Increase in Ransomware Attacks

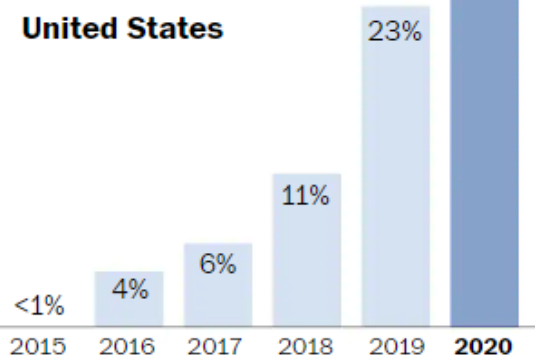
## Ransomware attacks are becoming more common in the United States

Ransomware accounted for 30% of all U.S.-based cyberattacks reported to and confirmed by Verizon data breach researchers in 2020, more than double the rate for the world.

### World



### United States



Source: Verizon 2021 Data Breach Investigations Report



**IN ADDITION TO THE INCREASE IN  
RANSOMWARE WE ARE SEEING A  
LARGE AMOUNT OF PHISHING ATTACKS  
TARGETING WIRE TRANSFER FRAUD!**

*Wire transfer fraud is estimated to be the fastest growing cyber-crime (according to the US Internet Crime Complaint Center). It targets individuals and businesses of all sizes.*

Land O'Lakes annually trains all employees who deal with Wire Transfer activities on LOL process and how to identify potential fraudulent activities – has resulted in significant increase in reporting of incidents and reduction in financial loss.



# Look-a-like Domains go up on a Regular Basis

landolakes.com.sc    landolakes.com    landolake.com

lolofeed.com    landolakes.com    landolakes.com

landolakes.com    landolakes.com    landolakes.com

landolakesinc.com    landolakes.com    landolakes.com

Spooferd LOL domains  
are often used to target  
our business partners –  
11X increase over 2021!

Takes careful inspection to identify potential spoofed domain!



*Wire transfer fraud is estimated to be the fastest growing cyber-crime (according to the US Internet Crime Complaint Center). It targets individuals and businesses of all sizes. In 2017, the FBI received more than 301,000 complaints with more than \$1.4 billion in damages!*

Engaging law enforcement early is critical - although acceptance of the case relies on prosecutive merit.

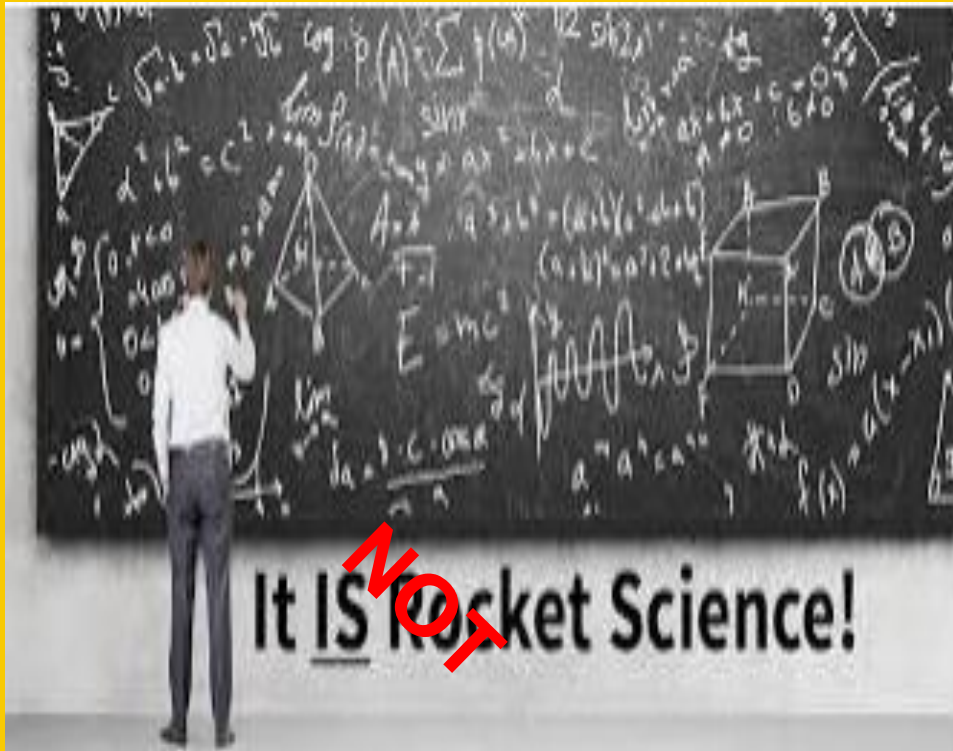


**“We’re too small”, they wouldn’t waste their time targeting us, right?**

Last year, small organizations accounted for less than half the number of breaches that large organizations showed.

This year these two are far closer with 307 breaches in large and 263 breaches in small organizations.





*“IT IS TEMPTING TO VIEW CYBERCRIMINALS AS EXTREMELY CLEVER, CAPABLE OF BREAKING THROUGH THE STRONGEST DEFENSES PUT IN FRONT OF THEM. THE REALITY IS THAT THEY OFTEN AREN’T, IF FOR NO OTHER REASON THAN THEY DON’T NEED TO BE.”*

Wire Transfer Fraud is not a technology issue – it’s a business process issue!





# The lifecycle of a wire-transfer hack



Fraudsters often target individuals that likely have the authority to perform wire transfers, CEO's, CFO's, Treasury, Finance individuals



It often starts with a phishing email to harvest that users credentials and gain access to their email system



They access your email and collect enough information to learn the types of billing the company pays, who the payee's are and the average balances paid.



They then spoof a customer or, in other words, take their identity, and bill the company with wire transfer instructions to a scam bank account often using a 'lookalike' domain name

Hacker's take their time, plan the actions out, and indicators are often 'slight' but 'noticeable' – you must be diligent and attentive in inspecting any such request to change banking information!



# The lifecycle of a wire-transfer hack



Fraudsters often target individuals that likely have the authority to perform wire transfers, CEO's, CFO's, Treasury, Finance individuals



It often starts with a phishing email to harvest that users credentials and gain access to their email system



They access your email and collect enough information to learn the types of billing the company pays, who the payee's are and the average balances paid.



They then spoof a customer or, in other words, take their identity, and bill the company with wire transfer instructions to a scam bank account often using a 'lookalike' domain name

Increased monitoring for Treasury & Finance

Security Awareness Training

Conditional access on all platforms

Monitor for spoofed domains; voice confirmation known source to validate change

Actions to Prevent Wire Fraud

# TYPICAL INDICATORS SOMETHING'S AMISS....

1. Small but noticeable spelling, grammatical or misuse of language in communications
2. A sense of urgency in getting payment – they often send repeated requests on status of wire
3. Email address domain spoofing – not always but often – takes careful inspection!
4. From address is a public domain email account – or doesn't match 'known' email address of sender
5. Phone number doesn't match company #

*Never trust the contents of an email to execute banking changes – ALWAYS call a 'known' number on file and confirm verbally and with a known resource!*



# Lack of Identity Protection is 80% of the Problem



# 80%

## IDENTITIES

80% of data breaches have a connection to compromised privileged credentials  
- FORRESTER RESEARCH

80% of breaches within hacking involve brute force or the use of lost or stolen credentials.  
- VERIZON DBIR 2020

*Human error attributes to 90+% of all breaches - phishing victims, poor password hygiene, using the same password, etc.*



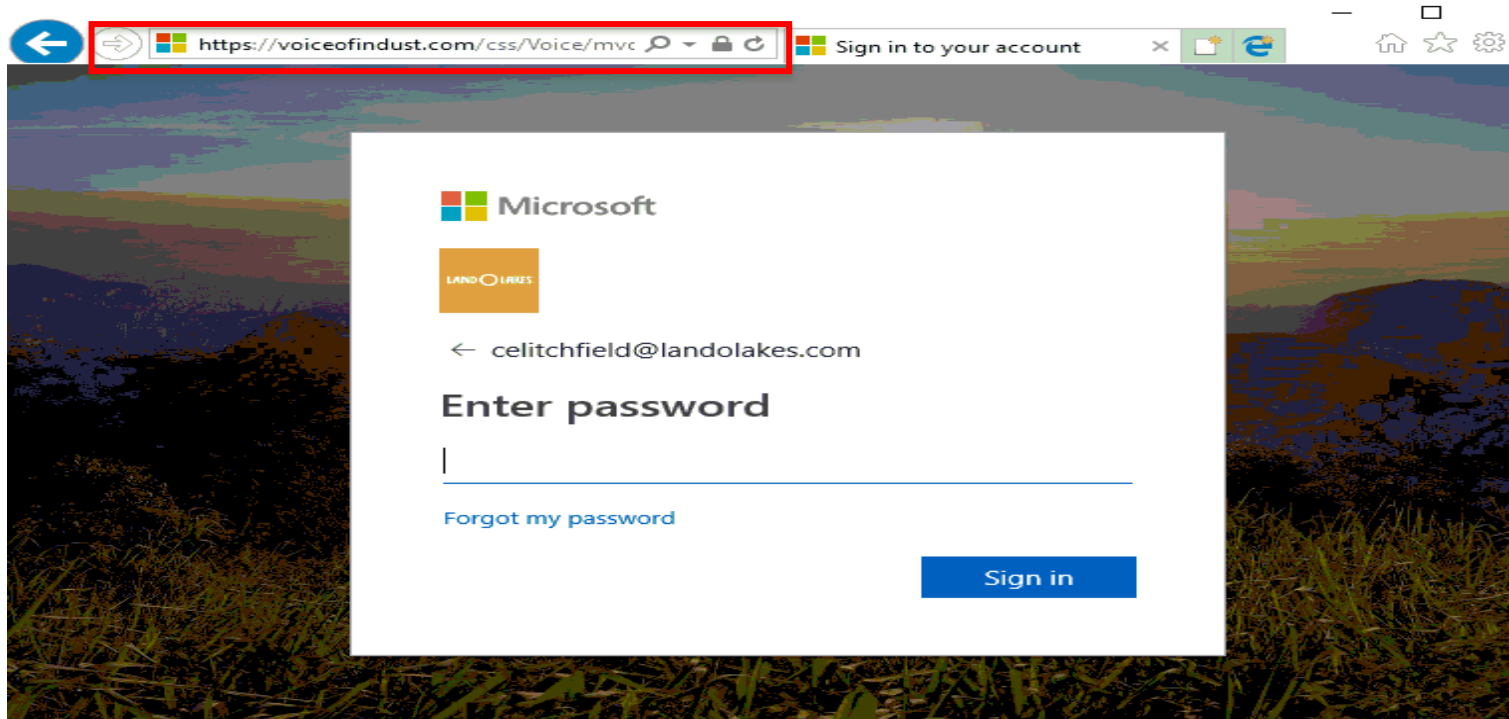
Threat actors only need 1 to succeed!





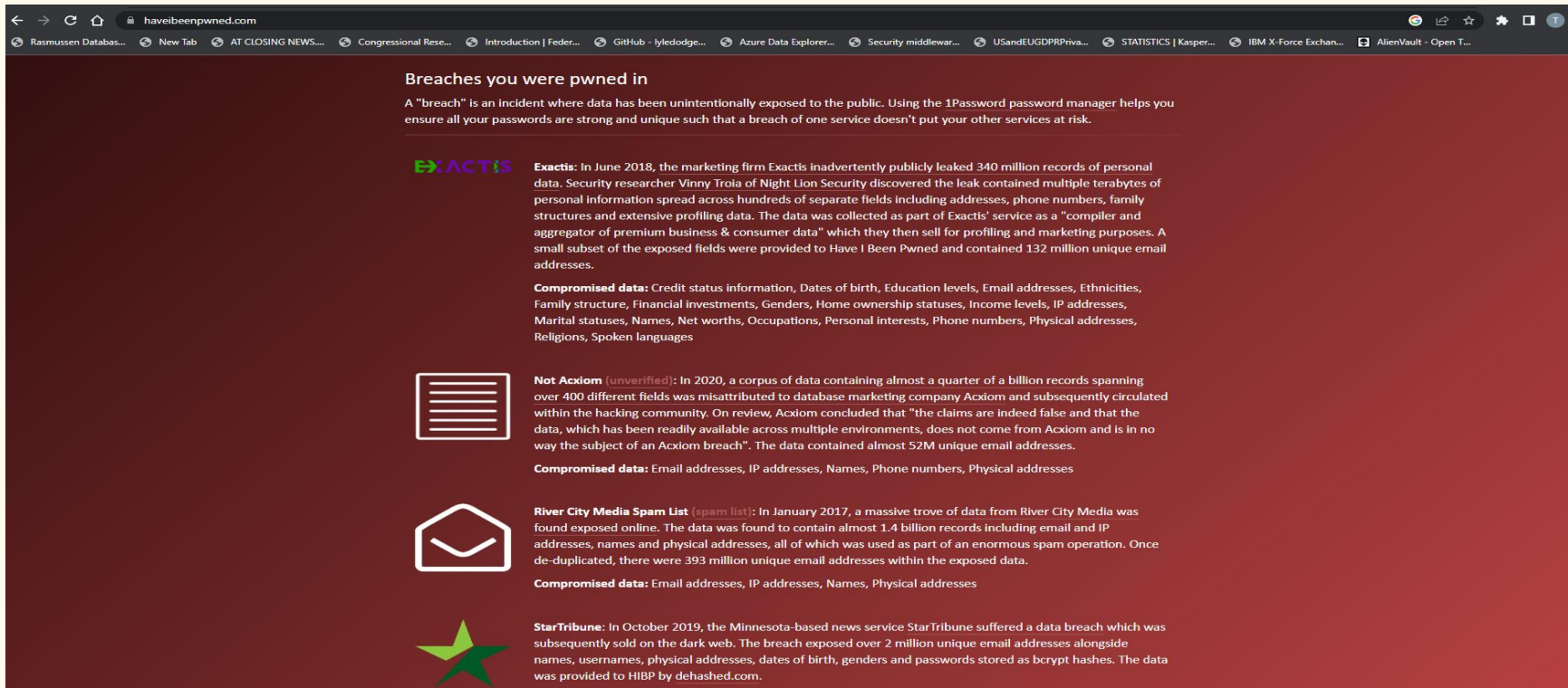
# The imposter's make it look real....

*Attempts to steal your identity abound*



# Many breaches start with a known breached password

Check your account - has it been breached by a 3<sup>rd</sup> party website?




**Breaches you were pwned in**


A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

**EXACTIS** **Exactis:** In June 2018, the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data. Security researcher Vinny Troia of Night Lion Security discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.


**Compromised data:** Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages

 **Not Acxiom (unverified):** In 2020, a corpus of data containing almost a quarter of a billion records spanning over 400 different fields was misattributed to database marketing company Acxiom and subsequently circulated within the hacking community. On review, Acxiom concluded that "the claims are indeed false and that the data, which has been readily available across multiple environments, does not come from Acxiom and is in no way the subject of an Acxiom breach". The data contained almost 52M unique email addresses.

**Compromised data:** Email addresses, IP addresses, Names, Phone numbers, Physical addresses

 **River City Media Spam List (spam list):** In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

**Compromised data:** Email addresses, IP addresses, Names, Physical addresses

 **StarTribune:** In October 2019, the Minnesota-based news service StarTribune suffered a data breach which was subsequently sold on the dark web. The breach exposed over 2 million unique email addresses alongside names, usernames, physical addresses, dates of birth, genders and passwords stored as crypt hashes. The data was provided to HIBP by dehashed.com.

# ***A LOOK AT A COUPLE 'REAL WORLD' EXAMPLES***





# REAL WORLD EXAMPLE OF WIRE FRAUD ATTEMPT

The attack began with a phishing email from a fake domain. Here's what that email looked like:

**From:** KATRINA DEVIN <katrina.devin@**elancoah.us**>  
**Sent:** Wednesday, November 9, 2022 12:28 PM  
**To:** AP Accounting <APAccounting@landolakes.com>;  
**Cc:** **@szlakelawfirm.com**>;  
**Subject:** Re: [EXTERNAL] Cancel Ach Payment (**URGENT**)  
**Importance:** High

Hi Katrina,

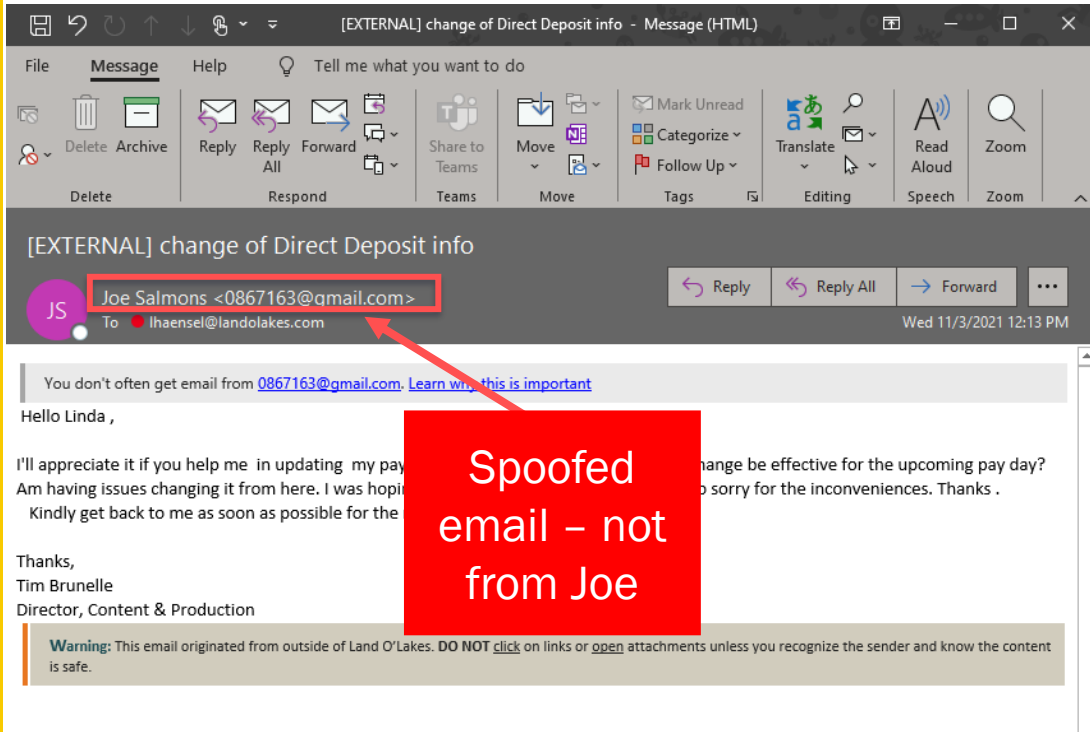
This is my third reminder, Elanco Animal Health will not be held liable for any loss of funds that may arise from the negligence/delay on the part of your team, **I have copied our Attorneys on this email**, attached is the **completed for like you requested. yesterday I wrote severally**, I am doing the same again today, kindly update our account and advise when completed.

Best,  
KATRINA

Here the perpetrator is impersonating Elanco with the fake 'elancoah.us' domain, as well as making threats to a fake law firm!



# DIRECT DEPOSIT SCAMS

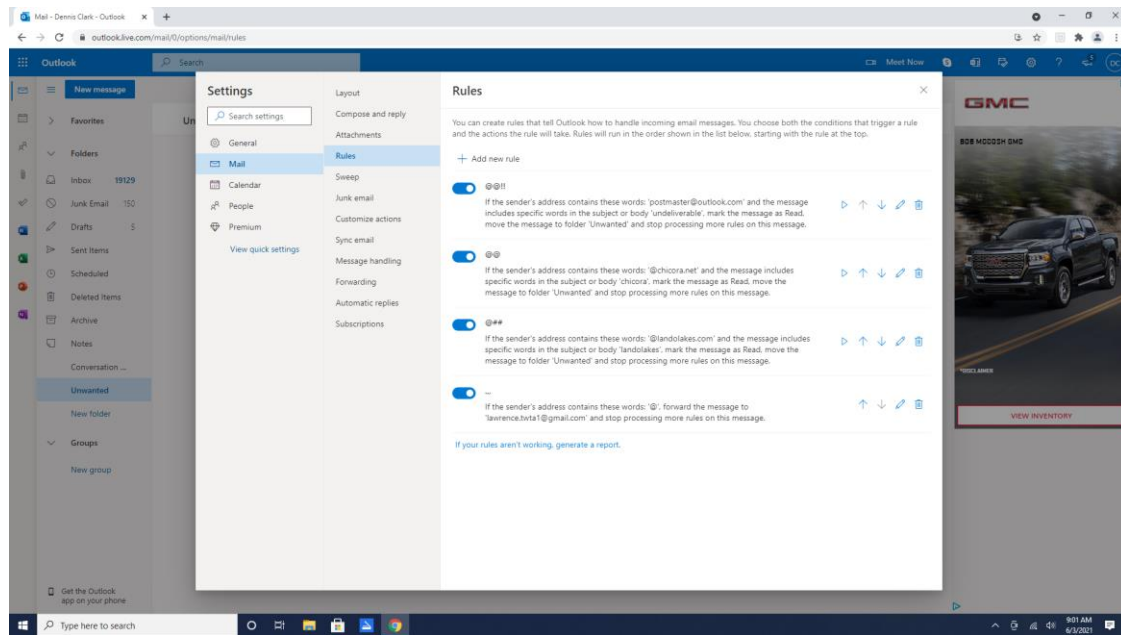


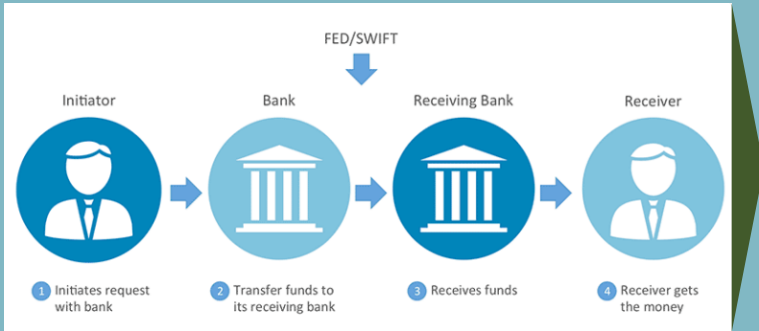
Unlike generic phishing scams, direct deposit scams – also known as payroll diversion scams – are specially crafted to the targeted organization. Threat actors impersonate an employee, often by establishing an email address using the employee's name and utilizing display name spoofing in the messages.



# ATTACKERS OFTEN INSERT INBOX RULES INTO COMPROMISED EMAIL ACCOUNTS TO HIDE THEIR ACTIONS

ONCE COMPROMISED A FULL INSPECTION OF YOUR EMAIL ACCOUNT IS REQUIRED





## Can a Wire Transfer Be Reversed?

The short answer: Not usually.

Domestic transfers between accounts at the same bank usually happen within 24 hours. But with the rise of digital banking, wire transfers process almost instantly.

Fraudsters can quickly receive the money, move it into another account, and vanish before the victims have time to cancel or reverse the transfer.

You can only reverse a wire transfer if the sending bank notifies the receiving bank of your cancellation request *before* the receiving bank processes the transfer. Once the receiving bank accepts the funds, you cannot reverse the transaction.

On international wire transfers, there is a small window of about 30 minutes during which you could potentially recall the funds. However, a reversal is only permitted in specific circumstances:

- Your bank made an error with the recipient's account number.
- The recipient received a higher amount of money than you intended to send.
- It was a duplicate transfer.

In these cases when the bank is at fault, your bank representatives are more likely to help. But if you made a mistake and seemingly authorized the transfer from your device or number, it's unlikely that the wire transfer can be reversed.



# THINK YOU MAY BE A VICTIM – DO THIS NOW!

## Step 1: Contact your IT Department

- *Many wire transfer fraud cases include a Business Email Compromise and/or spoofed 'look-a-like' domains.*
- *The threat actor may have gained access to your email system and may still be active in your environment.*
- *You're IT team will want to begin their own investigation immediately and ensure they get the hacker out of your environment.*
- *Do not use the email of the internal victim – their email may be compromised and seen by the threat actor.*
- *Do not attempt to correspond with the threat actor and let them know you're on to them!*
- *Threat actors often install mailbox rules on the victim's account hiding their activity – automatically moving or deleting emails, forwarding to an external email address, etc..*



# THINK YOU MAY BE A VICTIM – DO THIS NOW!

## Step 2: Contact your bank and initiate a “SWIFT recall” on the wire transfer that left your account.

- *You first need to call your bank and let them know the transfer you made was fraudulent and that you are requesting a SWIFT recall to be initiated. You must have all the information about the wire funds transfer in front of you to properly initiate this request.*
- *You also need to ask your bank to contact the fraud department of the receiving bank immediately so they can freeze the funds in the recipient account.*
- *Alternatively, if the funds—or part of the funds—have already been moved, you’ll need to ask the bank to find out where the money was sent. Ask them to contact the third bank (or banks) to freeze the accounts that received the money.*
- *Make a note of the banks and the accounts that received your money as you’ll need this information later.*



# THINK YOU MAY BE A VICTIM – DO THIS NOW!

## Step 3: File a complaint with the FBI's Internet Crime Complaint Center (IC3)

- *The next step is to contact the [FBI's Internet Crime Complaint Center](#). You'll need to provide information about the transaction, the scam itself, and the victim. It's a good idea to add details like the contents of the phishing email, links you clicked, etc. Once you have filed a complaint, the service will give you an IC3 Complaint Number. Make a note of this as you'll need it in step three.*
- *It's worth noting that filing a complaint with the FBI is necessary but does not guarantee a real-time recovery effort. It's up to you to complete the remaining steps to increase your chances of recovery. Be aware that the FBI is flooded with complaints like yours each and every day so you need to stay vigilant and be your own advocate for recovery.*



# THINK YOU MAY BE A VICTIM – DO THIS NOW!

## Step 4: Contact your local FBI field office and provide the IC3 complaint number

- Find your local [FBI field office at this link](#). You'll then need to contact them and report the details of the crime to the agent in charge of processing financial or cybercrimes. Following this, give them the IC3 Complaint Number and your personal contact information.
- If you're an enterprise, now's the time to contact legal counsel to determine if an injunctive order is necessary. If so, send the order to the banks involved. This will ensure that all banks that received your money are no longer able to transfer funds from such accounts.





# THINK YOU MAY BE A VICTIM – DO THIS NOW!

## Step 5: Contact all banks that may have also received your funds

- *If the fraudsters manage to transfer your money to another bank (or banks), you now must contact these banks. Ask to speak to their fraud department about requesting a SWIFT recall and a 'fraud freeze' on the recipient accounts.*
- *You'll have to provide information about the fraudulent transfers so the banks can identify the transfer and the account. Once the account is frozen, confirm with the bank how long the freeze will remain in place and that the SWIFT recall protocol has been initiated.*
- *Alternatively, if the money has already been moved on to a fourth bank account, you'll need to follow the same steps as above. You can even request the first bank you visit to send SWIFT recall and 'fraud freeze' requests to all other banks in the chain.*
- *Don't only rely on them though. Repeat the steps until all the accounts that received your money are frozen and that the SWIFT recall protocol is in process.*
- *Remember to write down the number you used to contact the bank, the time of the call, the name of the bank representative you spoke to, and their direct phone number and email address.*
- *If you're an enterprise or business, this is time to contact your insurance provider if you have errors and omissions coverage, professional liability coverage, or any form of cybersecurity or cyber loss coverage.*



# THINK YOU MAY BE A VICTIM – DO THIS NOW!

## Step 6: Contact local authorities and file a police report

- *Next, you need to contact the local authorities and file a police report. Give them all the information they may need.*
- *Save the incident number or police report number, and exchange contact information with local authorities for future communication.*



# KEY ASPECTS TO PROTECT AGAINST WIRE TRANSFER FRAUD

- **Trust no email** – if it's not spoofed and perfectly and legitimately from the company we're working with *you still can't trust it!* Business Email Compromise (BEC) is rampant and while many times the emails are spoofed, sometimes they are really from the company we expect but they've been compromised!
- **Trust no contact information** – don't trust the *signature line, their email, or their phone number*. Call ONLY a known good number to a known person to confirm legitimacy of any banking change request or new setup!
- **Use MFA for Email** – since many wire transfer fraud incidents begin with a phishing campaign to capture a user's credentials – MFA protects you from an account take-over, even if the employee was fooled into providing their credentials
- **Timing is of the essence** – if you think you've mistakenly wired money to a fraudulent account follow the actions identified previously ***immediately*** – *Bad News Does Not Get Better with Time!*



# WIRE TRANSFER BEST PRACTICES

*Wire Transfer Fraud is not a Technology Issue – it's a Process Issue!*

- Understanding email scams for wire-transfer fraud is rampant and educating your employees is critical to protect your financial assets.
- Requests for changes, immediate action, or lack of availability by phone should be met with intense scrutiny. Don't be pressured, slow down and follow established processes.
- Scrutinize all email correspondence regarding wiring funds: Who is requesting \$ and Why are they requesting \$.
- Do not use public domain email accounts (i.e. @gmail.com) for business purposes. Require wire transfer requests come from company domain email accounts when available.
- Implement dual control (2 people authorization) and segregation of duties - one person receives the request for funds, a second person authorizes the release of funds.
- Know your customers, their reasons for initiating or requesting wire transfers, and their habits regarding such wire transfers – if something seems 'off' it probably is!



*Always verify the authenticity of each wire transfer request by implementing a two-step verification process. Call the person, using a number you have previously called — not one from the current wire transfer request — to verbally verify it.*

# A LAYERED APPROACH TO MANAGING CYBER RESILIENCY

1. **MFA** – Multi-Factor Authentication in place for anyone accessing LOL network
2. **End Point protection** - Industry leading Malware protection + Vendor oversight
3. **Data Backups** - Extra layers of protection in place for data backups
4. **Vulnerability Management** - Regular scanning and patching
5. **Incident Response** – defined response, table-top exercises and professional retainer in place with industry experts
6. **Security Awareness** – Educating and training every employee on company policy and how to detect phishing
7. **Test Yourself** - validate your controls and detection capabilities via Red Team / Pen Test
8. **Wire Transfer Procedures** - two step authorization; verbal verification
9. **Manage Program Maturity** - NIST and CIS Top Twenty
10. **Federal Authorities** – plan ahead, know your local office and how to contact

Do the basics exceedingly well to address cyber resiliency – cyber criminals do not want to work any harder than necessary!



# SUMMARY

- We see nothing slowing cyber attacks or wire transfer fraud activities
- Attackers are well funded, typically organized crime or nation state actors.
- They target anyone and everyone and will move to the path of least resistance to capitalize on an attack.
- You must be continually looking to improve your operational efficacy to keep pace with the evolving threat landscape.



**Questions?**