

# ALTA

# inSIGHTS

REAL TIME | ON-DEMAND



## Cyber Security Trends and COVID-19

Tom Cronkright, Esq. | CertifID

Today's  
ALTA Insights  
Featured  
Sponsor



# Meet today's presenter



[tcronkright@certifid.com](mailto:tcronkright@certifid.com)

## Tom Cronkright

- Co-Founder and CEO, CertifID
- Licensed Attorney
- Large Title Agency Owner
- Wire Fraud Victim
- National Speaker on Wire Fraud and Cyber Security



# Today's Topics

- The Growth of Wire Fraud and COVID Scams
- Recent Fraud Examples
- Money Laundering and Wire Fraud Recovery
- Five Key Take-Aways



# Today's Topics

- **The Growth of Wire Fraud and COVID Scams**
- Recent Fraud Examples
- Money Laundering and Wire Fraud Recovery
- Five Key Take-Aways



# Poll Question #1



# PHISHING: The Top Tool in the Fraud Arsenal

+91%

Of all cyber attacks start  
with phishing

Source: PhishMe

+96%

Of groups' primary motivation  
is intelligence gathering

Source: Symatec's Internet Security Threat  
Report 2019

+400%

Number of incoming reports  
about hacking

Source: FBI



# PHISHING:

## Malicious and Compromised Email

+33%

of hacked  
accounts had  
dwelling over a  
week

Source: Barracuda – Spear  
Phishing: Top Threats and  
Trends Vol. 4

+45%

BEC attacks coming  
from malicious  
accounts

Source: Barracuda – Spear  
Phishing: Top Threats and  
Trends Vol. 4

+70%

BEC scams  
launched from free  
webmail accounts

Source: FBI



# PHISHING: Increasing Risk Profile

+148%

Increase in  
Ransomware  
Attacks in March  
from February '20

Source: VMware Carbon  
Black

+200%

Number of potentially  
compromised companies in U.S.  
in March from January '20

Source: Artic Security

+30,000%

Increase in COVID-  
related threats

Source: INFO Security



**A new phishing site launches  
every 20 seconds.**



# Recent FinCEN Advisory on COVID Scams



## FinCEN ADVISORY

FIN-2020-A005

July 30, 2020

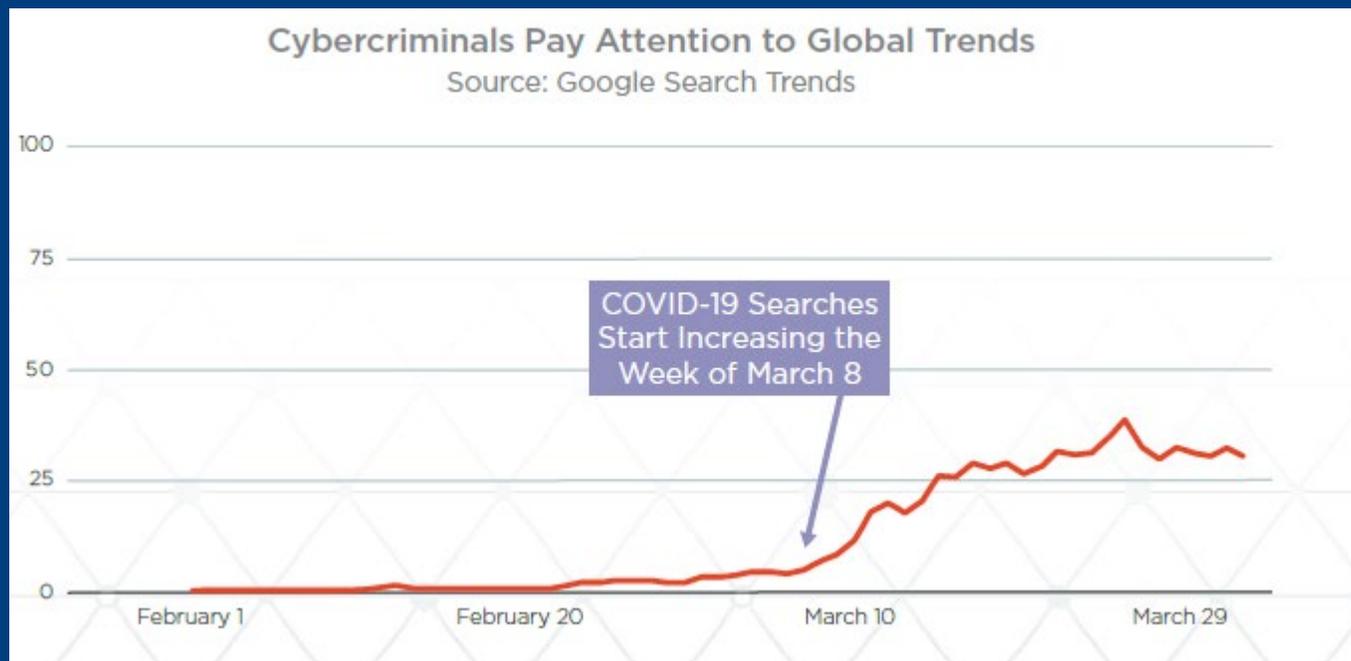
### Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic

*Detecting, preventing, and reporting illicit transactions and cyber activity will help protect legitimate relief efforts for the COVID-19 pandemic and help protect financial institutions and their customers against malicious cybercriminals and nation-state actors.*

FinCEN - <https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf>



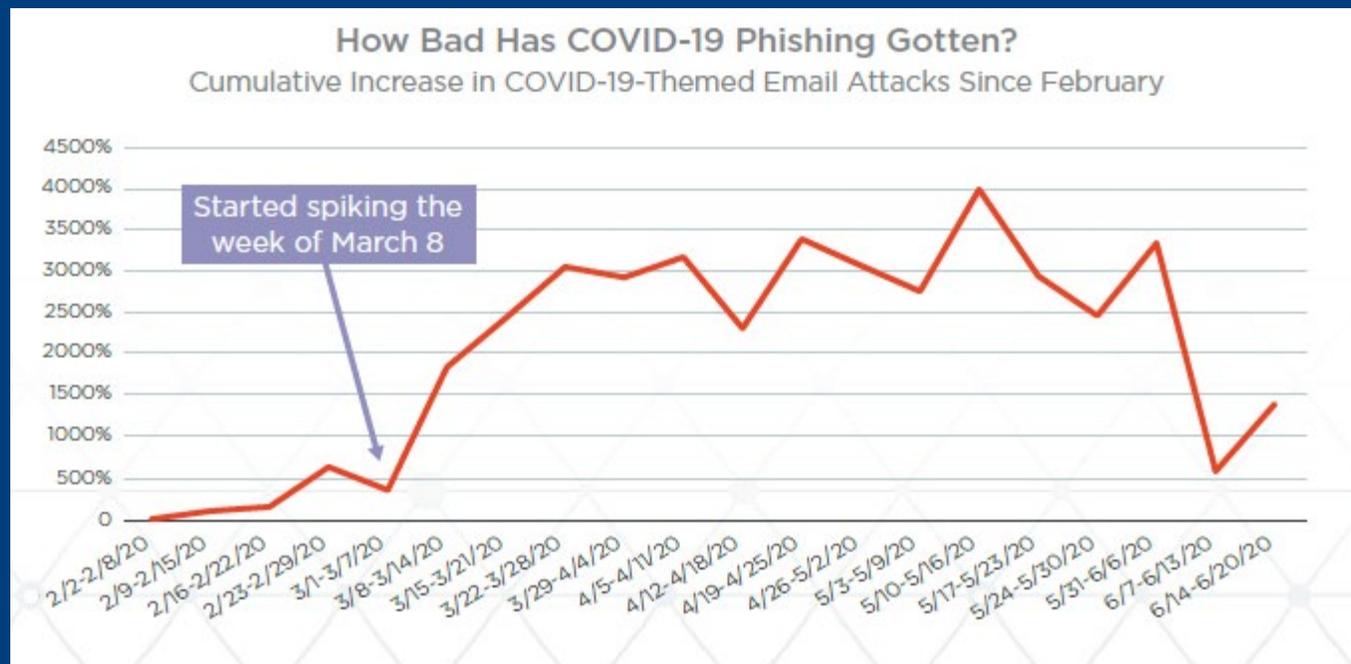
# COVID-Themed Phishing Attacks on the Rise



Source: Agari – H2 2020 Email Fraud & Identity Deception Trends



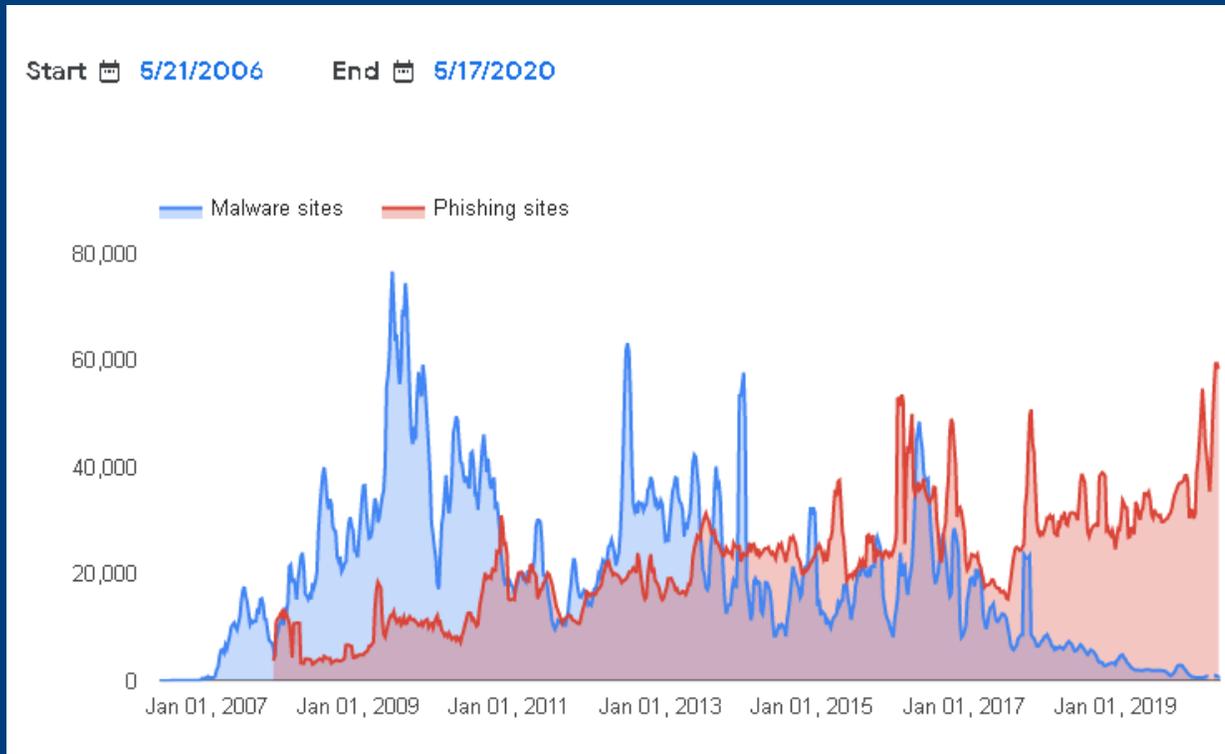
# COVID-Themed Phishing Attacks on the Rise



Source: Agari – H2 2020 Email Fraud & Identity Deception Trends



# Malware and Phishing Scams

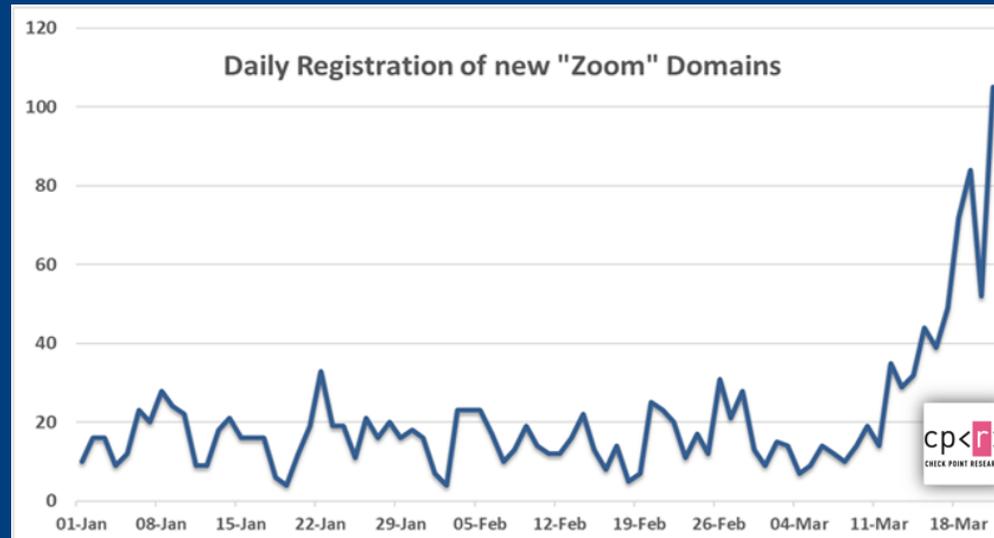


Source: Google



# “Zoom” Phishing

During the past few weeks, we have witnessed a major increase in new domain registrations with names including “Zoom”, which is one of the most common video communication platforms used around the world. **Since the beginning of the year, more than 1700 new domains were registered and 25% of them were registered in the past week.**

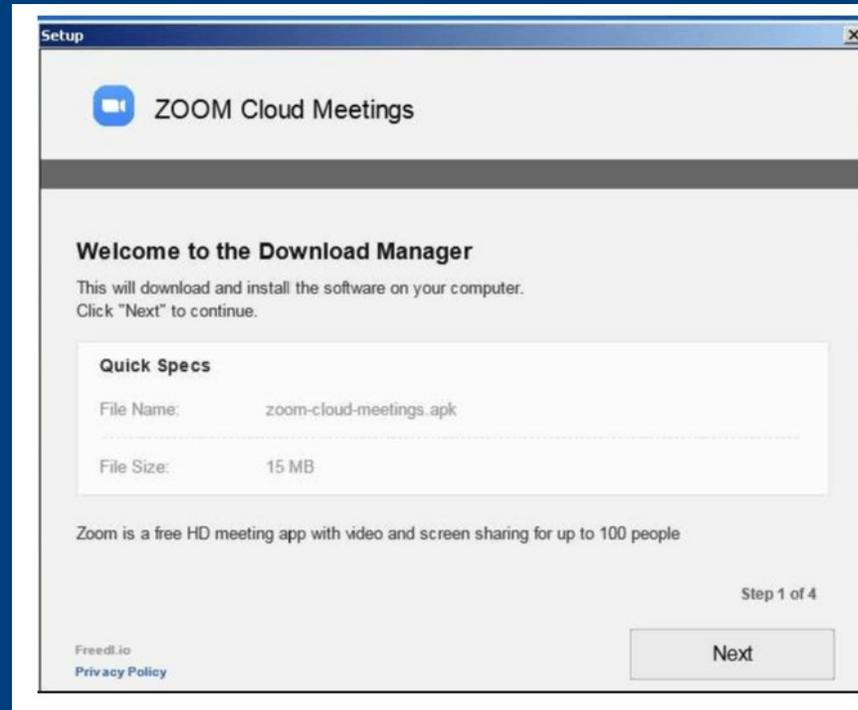


Source: Checkpoint Software Technologies

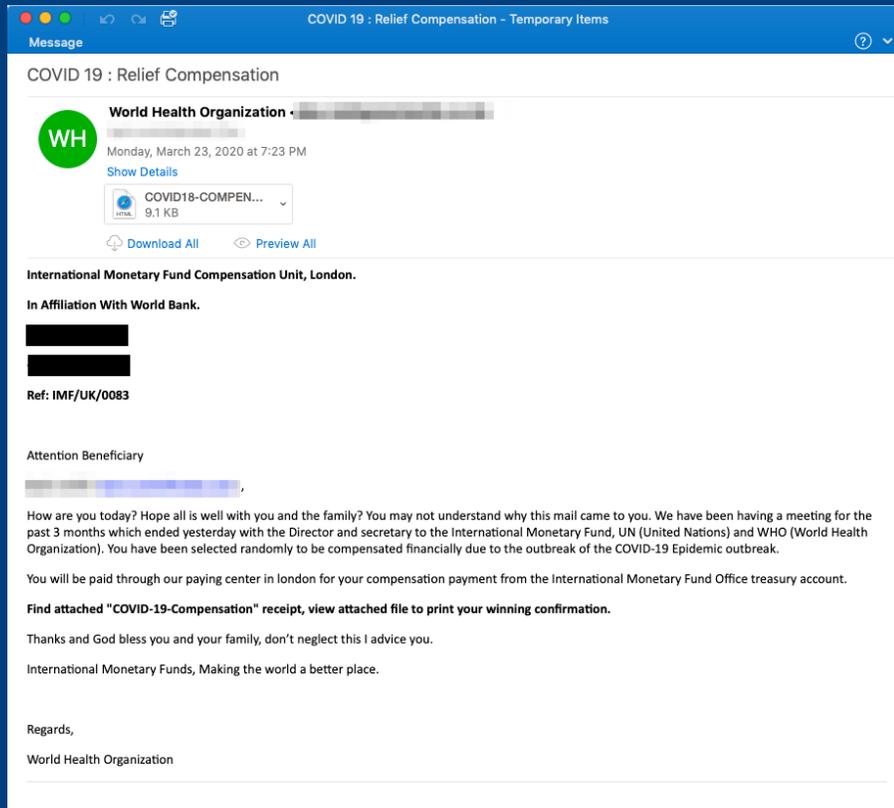


# “Zoom” Phishing

Malicious files with names such as “zoom-us-zoom\_#####.exe” and “microsoft-teams\_V#mu#D\_#####.exe” leads to an installation of the infamous InstallCore PUA (potentially unwanted applications) which could potentially lead to additional malicious software installation.



# Economic Relief from WHO and IMF

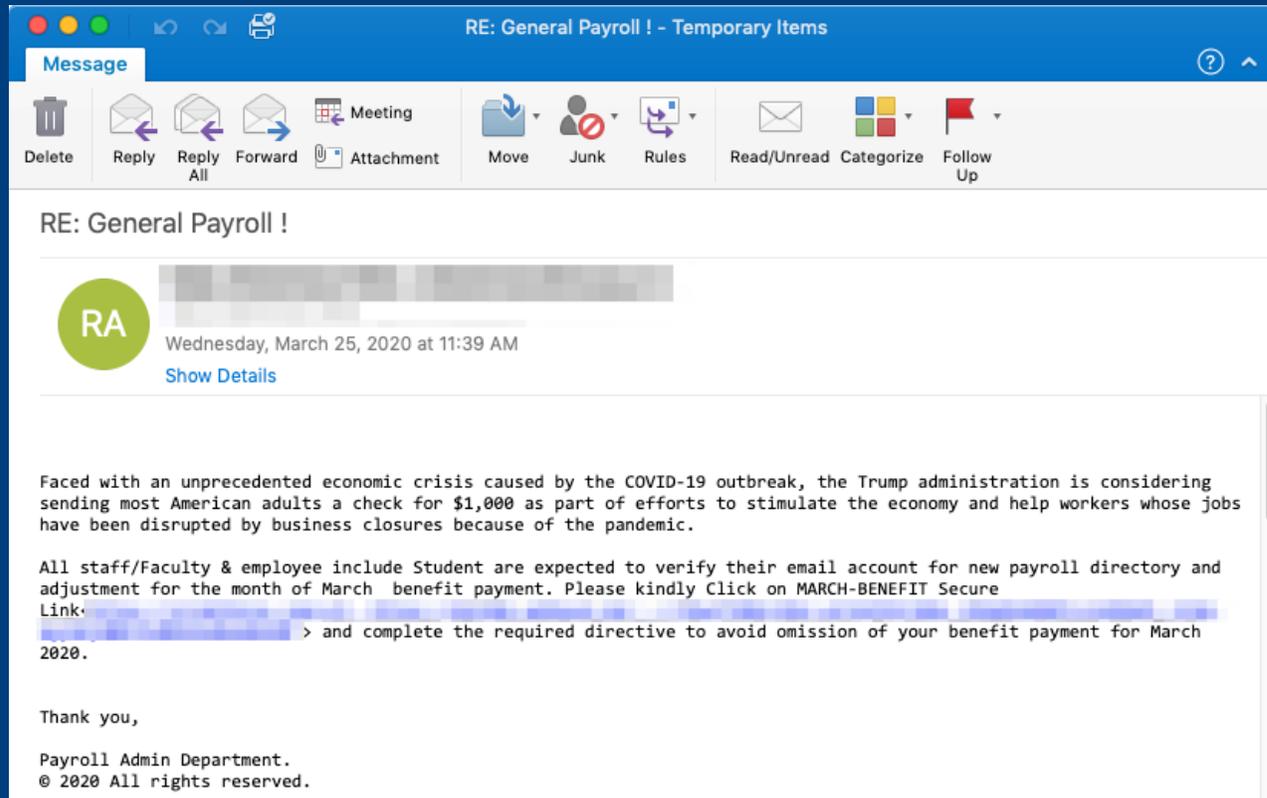


Source: Proofpoint

Issue: Malicious Microsoft Excel  
branded attachment that gathers  
emails and passwords.



# Trump Administration COVID-19 Benefits

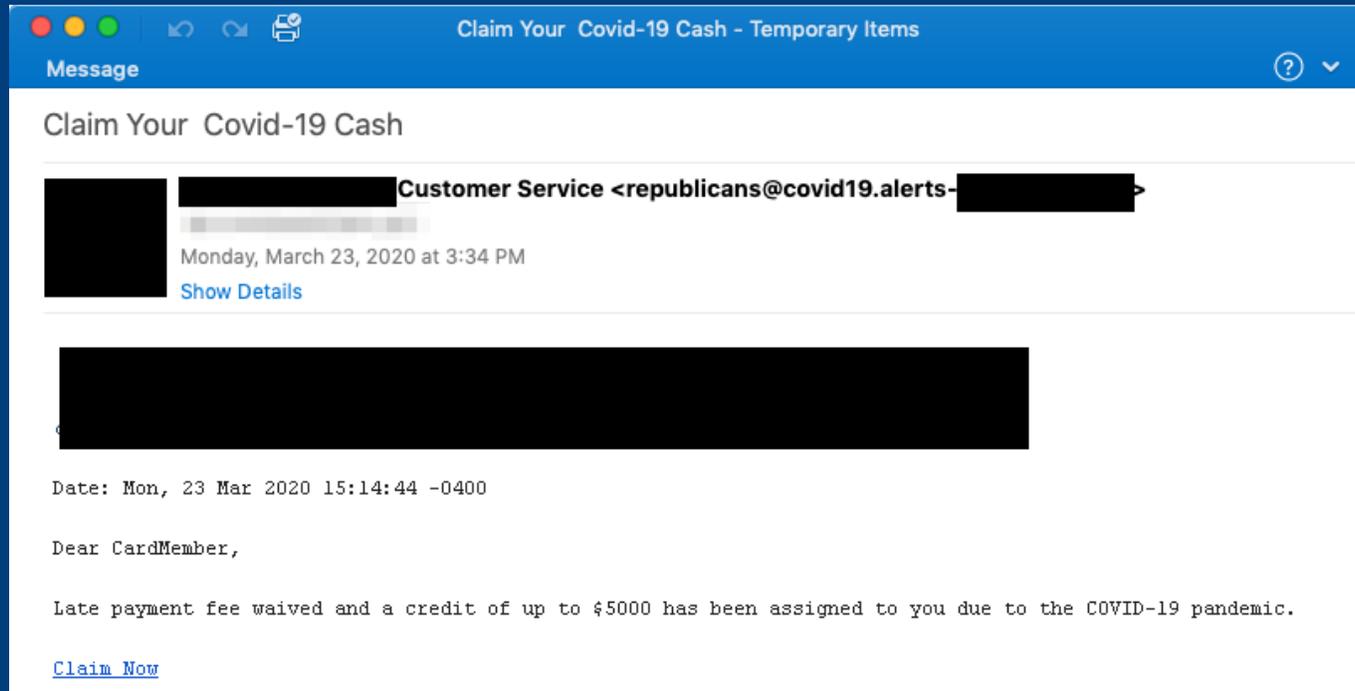


Source: Proofpoint

Issue: The email asks recipients to verify their email account through a malicious link that directs them to a phishing page.



# Credentials and Credit Card Phish



Source: Proofpoint

Issue: The email also contains a "Claim Now" link that takes the recipient to a spoofed page for the credit card company that attempts to steal the user's ID, password, email, credit card, and other details.



# Credentials and Credit Card Phish

Access Important Shared Document in regards to  
COVID-19 employee benefits review.

[Click To Add Documents To Office 365 OneDrive And View](#)

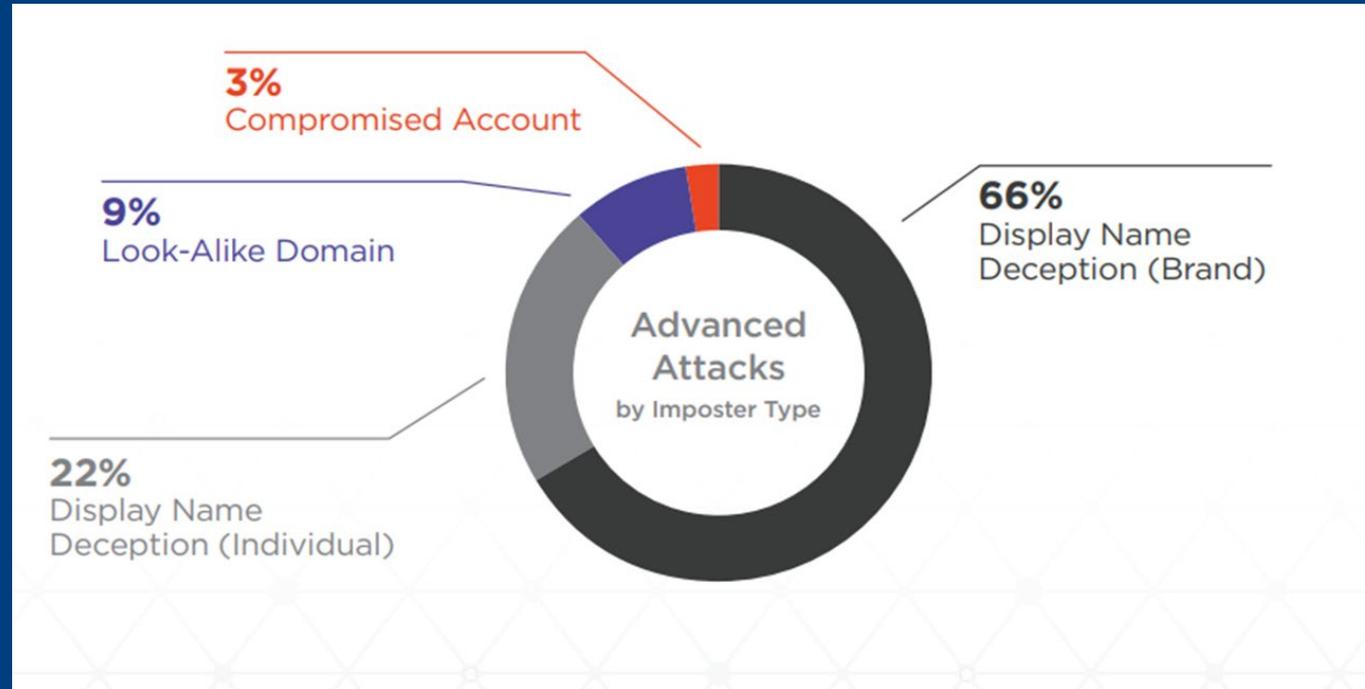
OneDrive by Microsoft makes creating and sharing seamlessly simple and secure.

Source: Menlo Security

Issue: Attachment contains malware that will install on device or network.



# Brand Impersonation is Top Phishing Strategy



Source: Agari – H2 2020 Email Fraud & Identity Deception Trends

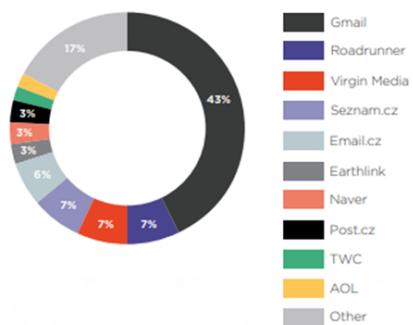


# Gmail is Top Email Platform for Phishing

## #1

### Gmail Remains The Most Weaponized Email Platform

Gmail accounts were used to launch 43% of all BEC scams, up from 35% since our last report.



Source: Agari – H2 2020 Email Fraud & Identity Deception Trends



# Why GMAIL?

- Quick to set up
- Free
- High reputational value to pass detection filters

Nearly 1/3 of all malicious GMAIL accounts are used for less than 24 hrs.



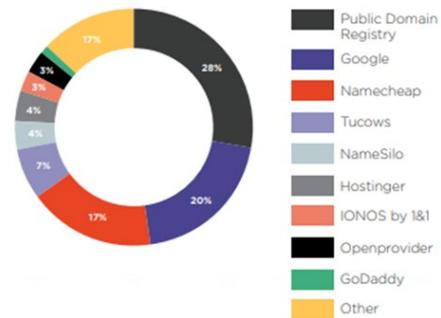
# Lookalike Domains Are Risky

**27%**

## BEC Emails Sent From Registered Lookalike Domains

Nearly 30% of BEC campaigns are launched from a domain registered by the attacker. Nearly two-thirds of these domains are registered with just three domain registrars:

- PublicDomainRegister (28%)
- Google (20%)
- Namecheap (17%)

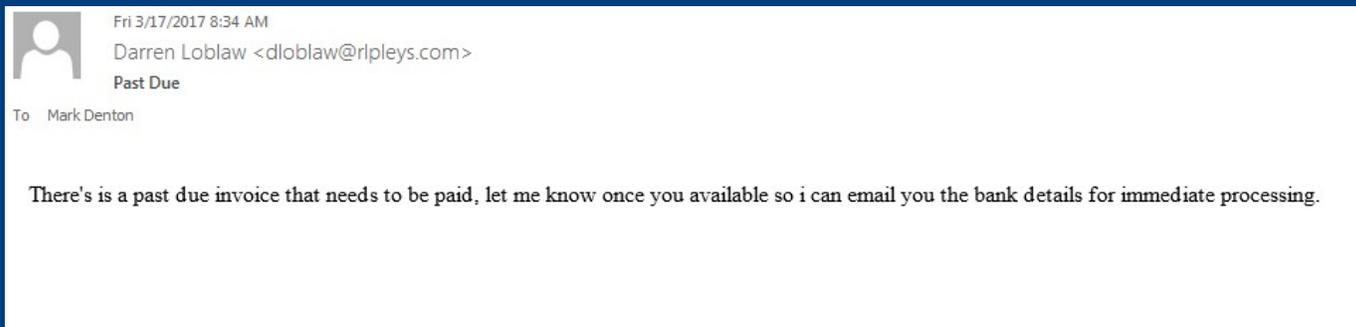


Source: Agari – H2 2020 Email Fraud & Identity Deception Trends



# Spoofered Domain Registrations





Real Domain : [hxxp://rpleys.com](mailto:hxxp://rpleys.com)

Spoofed Domain : [hxxp://rlpleys.com](mailto:hxxp://rlpleys.com)

“i” has been replaced with lowercase “l”

Business specifically targeted - Suspects know who to send the e-mail TO, how to address the message, and who to send the message FROM. Sent on 3/17/2017



# DomainTools Reverse WHOIS - “hxxp://www.rlpleys.com”

Registrant Name: John Edwin

Registrant Organization: foreslghtasg inc Registrant Street: 5800 THREE CHOPT RD

Registrant Street:

Registrant City: RICHMOND Registrant State/Province: VA Registrant Postal Code: 23226

Registrant Country: US

Registrant Phone: +1.9728780522 Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: don@foreslghtasg.com

Note: Domain registered and paid for at hxxp://1and1.com



# Additional Spoofed Domains registered by “don[[@](mailto:don@foresightasg.com)]foresightasg.com” via DomainTools

christywhlte.com -Legitimate – christywhite.com  
columbuszoo.org -Legitimate – columbuszoo.org  
nciinc.com -Legitimate – nciinc.com  
rpleys.com -Legitimate – rpleys.com  
rockwellcolliins.com -Legitimate – rockwellcollins.com  
turkeyhiil.com -Legitimate – turkeyhill.com

Domain Name	Create Date	Registrar
<a href="http://christywhlte.com">christywhlte.com</a>	2017-03-17	1&1 INTERNET SE
<a href="http://columbuszoo.org">columbuszoo.org</a>	2017-03-17	SCHLUND.DE
<a href="http://nciinc.com">nciinc.com</a>	2017-03-17	1&1 INTERNET SE
<a href="http://rpleys.com">rpleys.com</a>	2017-03-17	1&1 INTERNET SE
<a href="http://rockwellcolliins.com">rockwellcolliins.com</a>	2017-03-17	1&1 INTERNET SE
<a href="http://turkeyhiil.com">turkeyhiil.com</a>	2017-03-17	1&1 INTERNET SE



# WHOIS search on “hxxp://foreslghtasg.com” based on the email address of “don[@]foreslghtasg.com”

Registry Registrant ID: Registrant Name: James Fan

Registrant Organization: JPMORGAN INC Registrant Street: 10603 Lybert Rd Registrant Street:

Registrant City: Houston Registrant State/Province: TX Registrant Postal Code: 77041

Registrant Country: US

Registrant Phone: +1.9728780532

Registrant Phone Ext: Registrant Fax: Registrant Fax Ext:

Registrant Email: jjjmoreinc9090@mail.com

Domain registered and paid for at hxxp://1and1.com  
mail.com is a free-mail service



# Additional Spoofed Domains registered by “jjjmoreinc9090@mail.com”

arttherapystudio.org -Legitimate – arttherapystudio.org  
atlanticairnports.com -Legitimate – atlanticairnports.com  
decks-dockss.com -Legitimate – decks-docks.com  
foreslghtasg.com -Legitimate – foreslghtasg.com  
gemrc.com -Legitimate – gemrc.com  
idltrade.com -Legitimate – idltrade.com  
insrned.com -Legitimate – insrned.com  
locicontrols.com -Legitimate – locicontrols.com  
meritechcapital.com -Legitimate – meritechcapital.com

Domain Name	Create Date	Registrar
arttherapystudio.org	2017-03-15	--
atlanticairnports.com	2017-03-15	1&1 INTERNET SE
decks-dockss.com	2017-03-15	1&1 INTERNET SE
foreslghtasg.com	2017-03-15	1&1 INTERNET SE
gemrc.com	2017-03-15	1&1 INTERNET SE
idltrade.com	2017-03-15	1&1 INTERNET SE
insrned.com	2017-03-15	1&1 INTERNET SE
locicontrols.com	2017-03-15	1&1 INTERNET SE
meritechcapital.com	2017-03-15	1&1 INTERNET SE



# Initial Target (1)

ripleys.com -Legitimate – ripleys.com

# Additional Targets (14)

christywhite.com	-Legitimate – christywhite.com
columnbuszoo.org	-Legitimate – columbuszoo.org
nciinc.com	-Legitimate – nciinc.com
ripleys.com	-Legitimate – ripleys.com
rockwellcollins.com	-Legitimate – rockwellcollins.com
turkeyhill.com	-Legitimate – turkeyhill.com
arttherapystudio.org	-Legitimate – arttherapystudio.org
atlanticairports.com	-Legitimate – atlanticairports.com
decks-docks.com	-Legitimate – decks-docks.com
foresightasg.com	-Legitimate – foresightasg.com
gemrc.com	-Legitimate – gemrc.com
idtrade.com	-Legitimate – idtrade.com
insmed.com	-Legitimate – insmed.com
locicontrols.com	-Legitimate – locicontrols.com
meritechcapital.com	-Legitimate – meritechcapital.com



From: Paul Dillahay [<mailto:pdillahay@nciinc.com>]

Sent: Friday, March 17, 2017 9:10 AM

To: Narel, Lucas <[lnarel@NCIINC.com](mailto:lnarel@NCIINC.com)>

Subject: NCI, Inc

There's is a past due invoice that needs to be paid, let me know once you available so i can email you the bank details for immediate processing.

NCI INC reported they received an email from a spoofed domain targeting one of their personnel from spoofed domain “@NCIINC.COM”

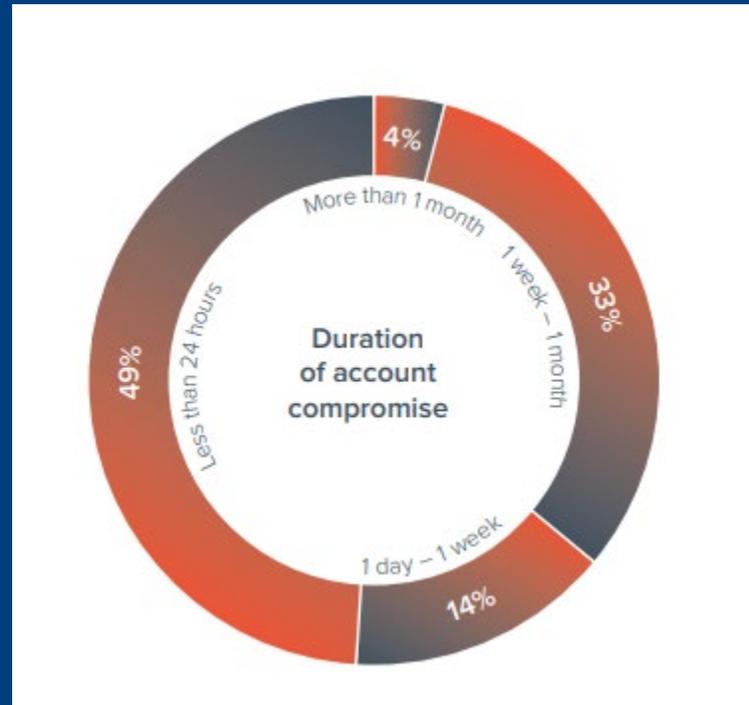
Business specifically targeted - Suspects know who to send the e-mail TO, how to address the message, and who to send the message FROM.



# Email Account Compromise



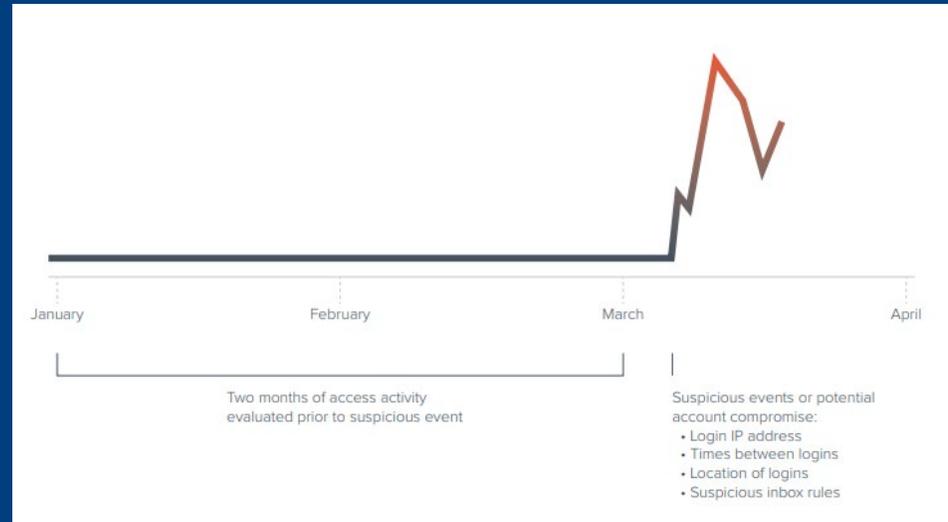
# Fraudsters Harvest Information Quickly



Source: Barracuda – Spear Phishing: Top Threats and Trends Vol. 4



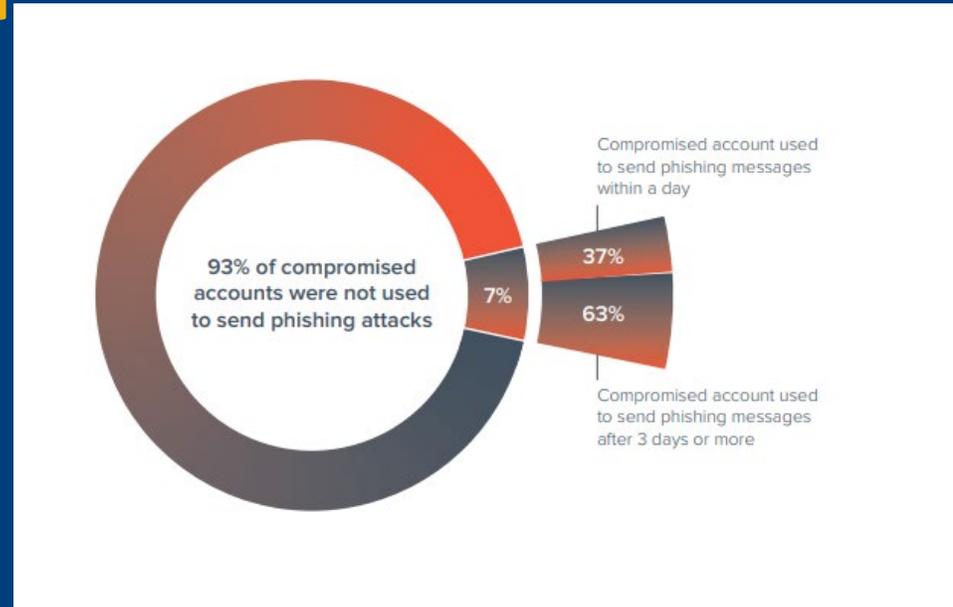
# Abnormal Usage Activity Leaves Clues of Compromise



Source: Barracuda – Spear Phishing: Top Threats and Trends Vol. 4



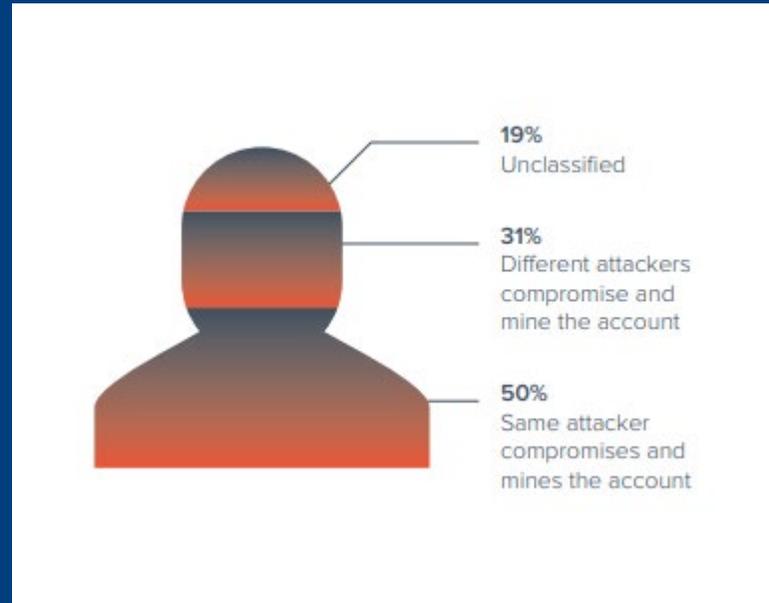
# Compromised Accounts Used to Harvest – Not Phish



Source: Barracuda – Spear Phishing: Top Threats and Trends Vol. 4



# Fraudsters Collaborate for Higher Impact



Source: Barracuda – Spear Phishing: Top Threats and Trends Vol. 4



# Today's Topics

- The Growth of Wire Fraud and COVID Scams
- **Recent Fraud Examples**
- Money Laundering and Wire Fraud Recovery
- Five Key Take-Aways



# Poll Question #2



# Fraud 1: Buyer Cash to Close

## Parties Involved



Commercial Real Estate Broker



Escrow Officer



Spoofed Escrow Officer



# Fraud 1: Buyer Cash to Close

**From:** [REDACTED]  
**Sent:** Friday, May 15, 2020 8:11 PM  
**To:** Renee M. VanDriel  
**Subject:** 725 36th

**\*\*EXTERNAL EMAIL\*\***

Hi Renee: The Seller for the property at 725 36th S W , Wyoming, Mi. wants to know if the attached resolution meets your approval if signed.  
Thanks  
[REDACTED]

On May 18, 2020, at 8:34 AM, Renee M. VanDriel <[rvandriel@suntitle.com](mailto:rvandriel@suntitle.com)> wrote:

Good morning [REDACTED]

Yes, it is acceptable.

Thankyou

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)

CORONAVIRUS NOTICE: If you are scheduled for a closing or plan to visit one of our offices, please postpone or reschedule your visit if you have any symptoms which may be similar to Coronavirus (fever, cough, shortness of breath, etc.) or have been in close proximity to someone who has these symptoms. We have alternative arrangements we can use for signing and delivering documents. Here is a link to our current protocols relating to Coronavirus: [www.suntitle.com/coronavirus](http://www.suntitle.com/coronavirus)

**\*\*\*WIRE FRAUD ALERT\*\*\*** We only deliver our wiring instructions to buyers and sellers through CertfID, an identity verification and bank account confirmation system ([www.certfid.com](http://www.certfid.com)). If you are a buyer or seller, you should NEVER accept wiring instructions from any other source or any other party to the transaction. Our wiring instructions never change – if you receive "new" wiring instructions, DO NOT USE THEM, and contact our office immediately using the phone number on our website. Everyone should protect themselves by verifying any wiring instructions via CertfID (or similar methods) or using a telephone number that is independently verified from a source other than the proposed wiring instructions.

The information contained in the preceding message is intended for viewing by the named addressee(s) only. This transmission may contain information that is privileged or otherwise confidential and is not intended for transmission to, or receipt by, anyone other than the named addressee(s). This transmission should not be copied or forwarded to anyone other than the named addressee(s). If you have received this transmission in error, please destroy and delete it from your system without copying or forwarding it, and notify the sender of the error by calling the phone number listed above.

**From:** [REDACTED]  
**Sent:** Monday, May 18, 2020 10:23 AM  
**To:** Renee M. VanDriel  
**Subject:** Re: 725 36th

**\*\*EXTERNAL EMAIL\*\***

So they can sign it and bring it to close? How does next week Friday look for a closing? Thanks [REDACTED]  
Sent from my iPhone



# Fraud 1: Buyer Cash to Close

On Monday, May 18, 2020, 03:44:45 PM GMT+1, Renee M. VanDriel <[rvandriel@suntitle.com](mailto:rvandriel@suntitle.com)> wrote:

The 29<sup>th</sup> works for me. What time?



Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)

**CORONAVIRUS NOTICE:** If you are scheduled for a closing or plan to visit one of our offices, please postpone or reschedule your visit if you have any symptoms which may be similar to Coronavirus (fever, cough, shortness of breath, etc.) or have been in close proximity to someone who has these symptoms. We have alternative arrangements we can use for signing and delivering documents. Here is a link to our current protocols relating to Coronavirus: [www.suntitle.com/coronavirus](http://www.suntitle.com/coronavirus)

**\*\*\*\*WIRE FRAUD ALERT\*\*\*\*** We only deliver our wiring instructions to buyers and sellers through **CertifiD**, an identity verification and bank account confirmation system ([www.certifid.com](http://www.certifid.com)). If you are a buyer or seller, you should NEVER accept wiring instructions from any other source or any other party to the transaction. Our wiring instructions never change – if you receive “new” wiring instructions, **DO NOT USE THEM**, and contact our office immediately using the phone number on our website. Everyone should protect themselves by verifying any wiring instructions via **CertifiD** (or similar methods) or using a telephone number that is independently verified from a source other than the proposed wiring instructions.

The information contained in the preceding message is intended for viewing by the named addressee(s) only. This transmission may contain information that is privileged or otherwise confidential and is not intended for transmission to, or receipt by, anyone other than the named addressee(s). This transmission should not be copied or forwarded to anyone other than the named addressee(s). If you have received this transmission in error, please destroy and delete it from your system without copying or forwarding it, and notify the sender of the error by calling the phone number listed above.

----- Forwarded Message -----

**From:** Renee M VanDriel <[rvandriel@suntitle.com](mailto:rvandriel@suntitle.com)>  
**To:** [REDACTED]  
**Sent:** Tuesday, May 19, 2020, 10:35:53 AM EDT  
**Subject:** Re: 725 36th



Good morning [REDACTED]

Kindly advise on the chosen time for closing on the 29th so we can schedule this closing thank you.

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)

**CORONAVIRUS NOTICE:** If you are scheduled for a closing or plan to visit one of our offices, please postpone or reschedule your visit if you have any symptoms which may be similar to Coronavirus (fever, cough, shortness of breath, etc.) or have been in close proximity to someone who has these symptoms. We have alternative arrangements we can use for signing and delivering documents. Here is a link to our current protocols relating to Coronavirus: [www.suntitle.com/coronavirus](http://www.suntitle.com/coronavirus)

**\*\*\*\*WIRE FRAUD ALERT\*\*\*\*** We only deliver our wiring instructions to buyers and sellers through **CertifiD**, an identity verification and bank account confirmation system ([www.certifid.com](http://www.certifid.com)). If you are a buyer or seller, you should NEVER accept wiring instructions from any other source or any other party to the transaction. Our wiring instructions never change – if you receive “new” wiring instructions, **DO NOT USE THEM**, and contact our office immediately using the phone number on our website. Everyone should protect themselves by verifying any wiring instructions via **CertifiD** (or similar methods) or using a telephone number that is independently verified from a source other than the proposed wiring instructions.

The information contained in the preceding message is intended for viewing by the named addressee(s) only. This transmission may contain information that is privileged or otherwise confidential and is not intended for transmission to, or receipt by, anyone other than the named addressee(s). This transmission should not be copied or forwarded to anyone other than the named addressee(s). If you have received this transmission in error, please destroy and delete it from your system without copying or forwarding it, and notify the sender of the error by calling the phone number listed above.



# Fraud 1: Buyer Cash to Close

----- Forwarded Message -----

**From:** Renee M VanDriel <rvandriel@suntitle.com>

**To:** [REDACTED]

**Sent:** Wednesday, May 20, 2020, 8:08:17 AM EDT

**Subject:** [REDACTED] St.



[REDACTED],

Attached you will find a copy of the Final Hud for your Approval and our wire instructions for buyers funding towards closing also kindly advise buyer to make payment before closing date and send a receipt so we can get all arranged for a quick closing on the [REDACTED]. Please review and let me know of any changes thank you.

Thank you

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 [REDACTED] Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)



# Fraud 1: Buyer Cash to Close



## WIRE INSTRUCTIONS

**BANK NAME:** Chase Bank  
570 broad St Ste  
110 Newark, NJ 07102

**ACCOUNT NAME:** Sun Title Agency

**ACCOUNT NO:** 612866282

**ROUTING NO:** 021000021

**ADDRESS:** 1410 Plainfield Ave., N.E. Grand Rapids, MI 49506



# Fraud 1: Buyer Cash to Close

**From:** Renee M VanDriel <rvandriel@suntitle.com>

**To:** [REDACTED]

**Sent:** Friday, May 22, 2020, 11:45:09 AM EDT

**Subject:** Re: Buyer's statement



Good Morning [REDACTED],

Kindly advise when we would be receiving buyers wire since we don't have the buyers contact. I believe you have advised Them to make the wire to our firms escrow account before closing, so we can get all documents organised and have a quick closing on the 29th thank you.

Best Regards,

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)



# Fraud 1: Buyer Cash to Close

On Friday, May 22, 2020, 04:55:18 PM GMT+1, [REDACTED] > wrote:



I reviewed and gave the Buyer the letter you furnished with wire instructions. I think she will wire it before noon on Tuesday the [REDACTED]. I told her to call me as soon as she had sent it so I could tell you. Have a great holiday  
[REDACTED]



# Fraud 1: Buyer Cash to Close

On Friday, May 22, 2020, 05:03:36 PM GMT+1, Renee M VanDriel <[rvandriel@suntitle.com](mailto:rvandriel@suntitle.com)> wrote:



Thanks for the update [REDACTED], Have a nice weekend and Holiday with your family. I will be keeping in touch thank you.

Best Regards,

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)



# Fraud 1: Buyer Cash to Close

----- Forwarded Message -----

**From:** Renee M VanDriel <rvandriel@suntitle.com>  
**To:** [REDACTED]  
**Sent:** Monday, May 25, 2020, 9:19:15 AM EDT  
**Subject:** Re: Buyer's statement



Good Morning [REDACTED]

Happy Memorial Day, We are closing on another property today and buyer already wired the purchase amount of \$858,000 Into our firms account, as advised by our accounting your own buyers wire should go out to our firms second account which wire instructions are attached here also for payment not to get mixed up for both closings. Kindly confirm you are in receipt and update [REDACTED] for payment tomorrow thank you.

Best Regards,

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)



# Fraud 1: Buyer Cash to Close



## WIRE INSTRUCTIONS

BANK NAME: Wells Fargo  
9200 Westheimer Rd,  
Houston Tx

ACCOUNT NAME: Sun Title Agency

ACCOUNT NO: 8901343858

ROUTING NO: 121000248

ADDRESS: 1410 Plainfield Ave., N.E. Grand Rapids, MI 49506



# Fraud 1: Buyer Cash to Close

On Monday, May 25, 2020, 02:36:52 PM GMT+1, [REDACTED] wrote:



I will tell them. I don't think they have wired any money yet. They have money in two banks, so will probably wire money from Chase Bank and from Flagstar bank. I had told them to make sure to have it wired before noon on [REDACTED]. When wired they are to call me so I can tell you it has been wired. See you at [REDACTED] morning.

Enjoy the day with your family

Thanks

[REDACTED]



# Fraud 1: Buyer Cash to Close

**FW: Buyer's statement - Fraud**

Renee M. VanDriel  
To: Tom Cronknight

Retention Policy: Executive-Entire-Mailbox-Permanently-1-year (1 year)  
Expires: 5/25/2021

You forwarded this message on 5/29/2020 1:11 PM.

Sun Title Wire Instructions.pdf  
70 KB

Bing Maps

Fraud email.

Renee VanDriel  
Commercial Escrow Officer  
Sun Title Agency  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9100 x2470 Main Line  
(616) 458-9300 Fax  
[www.suntitle.com](http://www.suntitle.com)

CORONAVIRUS NOTICE: If you are scheduled for a closing or plan to visit one of our offices, please postpone or reschedule your visit if you have any symptoms which may be similar to Coronavirus (fever, cough, shortness of breath, etc.) or have been in close proximity to someone who has these symptoms. We have alternative arrangements we can use for signing and delivering documents. Here is a link to our current protocols relating to Coronavirus: [www.suntitle.com/coronavirus](http://www.suntitle.com/coronavirus)

**\*\*\*MRE FRAUD ALERT\*\*\*** We only deliver our wiring instructions to buyers and sellers through CertiID, an identity verification and bank account confirmation system ([www.certifid.com](http://www.certifid.com)). If you are a buyer or seller, you should NEVER accept wiring instructions from any other source or any other party to the transaction. Our wiring instructions never change – if you receive “new” wiring instructions, DO NOT USE THEM, and contact our office immediately using the phone number on our website. Everyone should protect themselves by verifying any wiring instructions via CertiID (or similar methods) or using a telephone number that is independently verified from a source other than the proposed wiring instructions.

The information contained in the preceding message is intended for viewing by the named addressee(s) only. This transmission may contain information that is privileged or otherwise confidential and is not intended for transmission to, or receipt by, anyone other than the named addressee(s). This transmission should not be copied or forwarded to anyone other than the named addressee(s). If you have received this transmission in error, please destroy and delete it from your system without copying or forwarding it, and notify the sender of the error by calling the phone number listed above.

From: Donald [REDACTED]  
Sent: Monday, May 25, 2020 9:47 AM  
To: Renee M. VanDriel  
Subject: Fw: Buyer's statement

**\*\*EXTERNAL EMAIL\*\***

----- Forwarded Message -----  
From: Renee M VanDriel <[rvandriel@suntitle.com](mailto:rvandriel@suntitle.com)>  
To: [REDACTED]  
Sent: Monday, May 25, 2020, 9:19:15 AM EDT



# Fraud 1: Buyer Cash to Close

----- Forwarded Message -----

**From:** Renee M VanDriel <rvandriel@suntitle.com>

**To:** [REDACTED]

**Sent:** Monday, May 25, 2020, 10:00:36 AM EDT

**Subject:** Re: Buyer's statement



Thanks for the update [REDACTED], kindly get the wire receipt from them and forward to my email after wire has been done tomorrow for payment confirmation.

Best Regards,

Renee VanDriel  
Commercial Escrow Officer  
**Sun Title Agency**  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)



**Result: \$54,000 was wired  
on Friday, May 22, 2020**



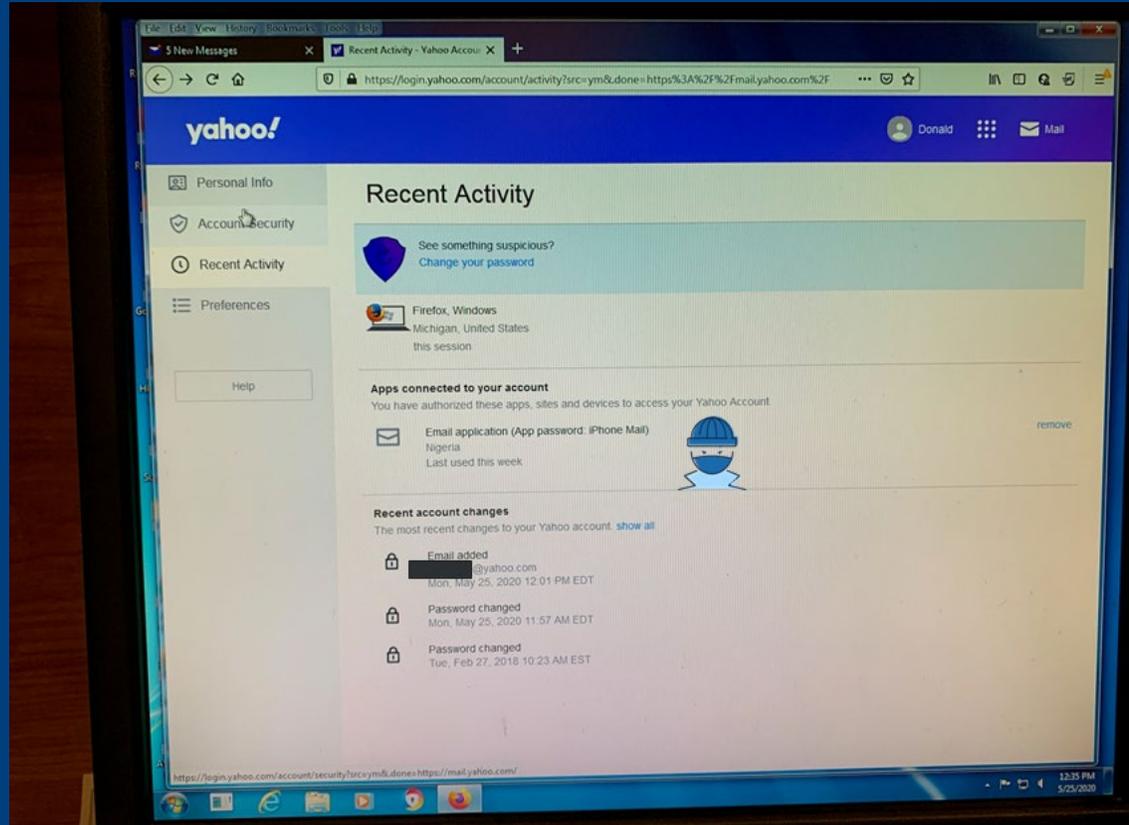
**How did they do it?**



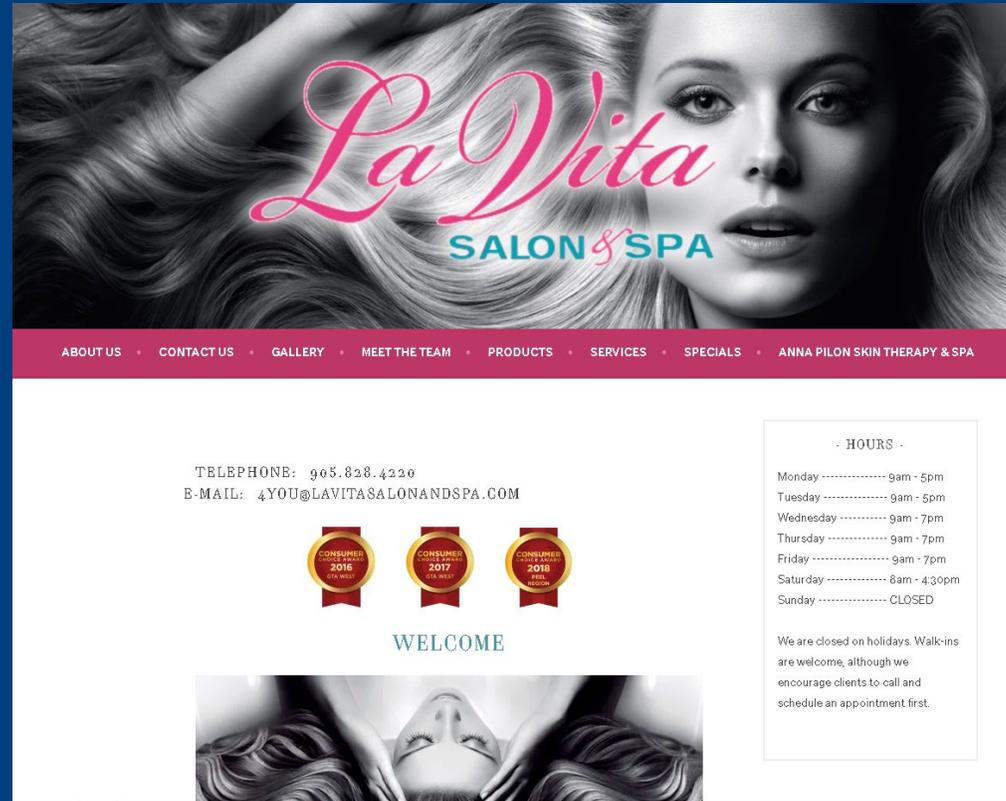
# Fraud 1: Broker Email Compromised



# Fraud 1: Broker Email Compromised



# Fraud 1: Mail server takeover



The screenshot shows the homepage of La Vita Salon & Spa. At the top is a large image of a woman's face with long, wavy hair. The text 'La Vita' is written in a pink cursive font, and 'SALON & SPA' is in a teal sans-serif font below it. A dark red navigation bar contains the following links: ABOUT US, CONTACT US, GALLERY, MEET THE TEAM, PRODUCTS, SERVICES, SPECIALS, and ANNA PILON SKIN THERAPY & SPA. Below the navigation bar, the contact information is listed: TELEPHONE: 905.828.4226 and E-MAIL: 4YOU@LAVITASALONANDSPA.COM. Three gold award medals are displayed, each with a ribbon and the text 'CONSUMER CHOICE AWARD' and a year (2016, 2017, and 2018). Below the medals is the word 'WELCOME' in teal. To the right of the 'WELCOME' text is a small image of a woman lying down with her hands near her face. On the far right of the page is a white box titled '- HOURS -' containing a list of days and their respective operating hours. Below the hours is a paragraph stating: 'We are closed on holidays. Walk-ins are welcome, although we encourage clients to call and schedule an appointment first.'

ABOUT US · CONTACT US · GALLERY · MEET THE TEAM · PRODUCTS · SERVICES · SPECIALS · ANNA PILON SKIN THERAPY & SPA

TELEPHONE: 905.828.4226  
E-MAIL: 4YOU@LAVITASALONANDSPA.COM

CONSUMER CHOICE AWARD 2016  
CONSUMER CHOICE AWARD 2017  
CONSUMER CHOICE AWARD 2018

WELCOME

- HOURS -

Monday	9am - 5pm
Tuesday	9am - 5pm
Wednesday	9am - 7pm
Thursday	9am - 7pm
Friday	9am - 7pm
Saturday	8am - 4:30pm
Sunday	CLOSED

We are closed on holidays. Walk-ins are welcome, although we encourage clients to call and schedule an appointment first.



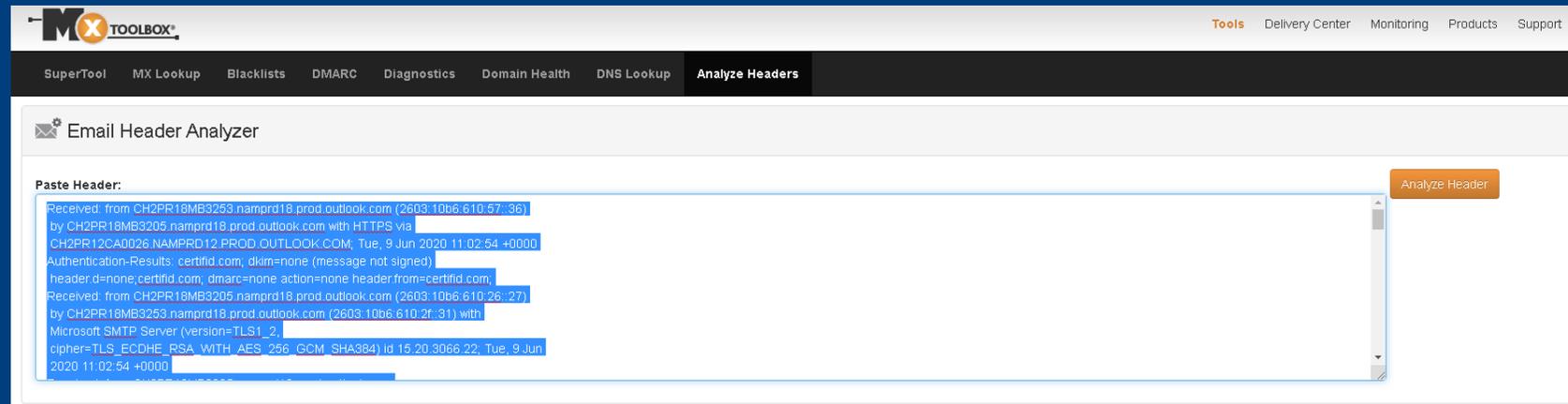
# Fraud 1: Spoofed Identity

The screenshot displays an email client interface with a sidebar on the left containing options like 'Info', 'Save', 'Save As', 'Save as Adobe PDF', 'Save Attachments', 'Print', 'Close', 'Office Account', 'Feedback', and 'Options'. The main area is titled 'Email header analysis' and includes several actions: 'Encrypt this item', 'Move item to a different folder', 'Message Delivery Report', 'Message Resend and Recall', and 'Properties'. The 'Properties' dialog box is open, showing settings for 'Importance' (Normal), 'Sensitivity' (Normal), and 'Security' options. The 'Internet headers' section is highlighted, showing the following text:

```
Received: from CH2PR18MB3253.namprd18.prod.outlook.com  
(2603:10b6:610:57::36)  
by CH2PR18MB3205.namprd18.prod.outlook.com with HTTPS via  
CH2PR12CA0026.NAMPRD12.PROD.OUTLOOK.COM; Tue, 9 Jun 2020  
11:02:54 +0000  
Authentication-Results: certifid.com; dkim=none (message not signed)  
header.d=none;certifid.com; dmarc=none action=none
```

A lightbulb icon is visible in the bottom right corner of the interface.

# Fraud 1: Spoofed Identity



The screenshot shows the MX Toolbox website's 'Email Header Analyzer' tool. The page has a dark blue header with the MX Toolbox logo and navigation links: Tools, Delivery Center, Monitoring, Products, and Support. Below the header is a dark navigation bar with links: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Domain Health, DNS Lookup, and Analyze Headers. The main content area is titled 'Email Header Analyzer' and features a 'Paste Header:' label and a large text input field. The input field contains the following email header text:

```
Received: from CH2PR18MB3253.namprd18.prod.outlook.com (2603:10b6:610:57:36)
by CH2PR18MB3205.namprd18.prod.outlook.com with HTTPS via
CH2PR12CA0026.NAMPRD12.PROD.OUTLOOK.COM, Tue, 9 Jun 2020 11:02:54 +0000
Authentication-Results: certfwd.com; dkim=none (message not signed)
header.d=none,certfwd.com; dmarc=none action=none header.from=certfwd.com;
Received: from CH2PR18MB3205.namprd18.prod.outlook.com (2603:10b6:610:26:27)
by CH2PR18MB3253.namprd18.prod.outlook.com (2603:10b6:610:2f:31) with
Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3066.22; Tue, 9 Jun
2020 11:02:54 +0000
```

To the right of the input field is an orange 'Analyze Header' button.



# Fraud 1: Spoofed Identity

Header-Name:	Header-Value:
X-Apparently-To:	[REDACTED]@yahoo.com; Mon, 25 May 2020 14:00:36 +0000
Return-Path:	<4you@lavitalonandspa.com>
Authentication-Results:	mta4196.mail.bf1.yahoo.com; dkim=neutral (no sig) header.i=@suntitle.com; spf=fail smtp.mailfrom=@lavitalonandspa.com; dmarc=NONE (p=NULL; sp=NULL; dis=NULL); header.from=suntitle.com;
Received-SPF:	fail (domain of lavitalonandspa.com does not designate 173.201.193.36 as permitted sender)
X-Originating-IP:	[173.201.193.36]
X-SECURESERVER-ACCT:	4you@lavitalonandspa.com
From:	"Renee M VanDriel" <rvandriel@suntitle.com>
X-Sender:	4you@lavitalonandspa.com
Reply-To:	"Renee M VanDriel" <rvandriel@suntitle.com>
To:	"Donald [REDACTED]" <[REDACTED]@yahoo.com>
Subject:	Re: Buyer's statement
Date:	Mon, 25 May 2020 07:00:01 -0700
Mime-Version:	1.0
X-Yahoo-Forwarded:	From: [REDACTED]@yahoo.com To: abwalant09@gmail.com



# Fraud 1: Spoofed Identity

```
X-Atlas-Received: from 10.201.196.220 by atlas320.free.mail.bf1.yahoo.com with http; Mon, 25 May 2020 14:00:36 +0000
X-Apparently-To: [REDACTED]@yahoo.com; Mon, 25 May 2020 14:00:36 +0000
Return-Path: <4you@lavitalonandspa.com>
Authentication-Results: mta4196.mail.bf1.yahoo.com;
dkim=neutral (no sig) header.i=@suntitle.com;
spf=fail smtp.mailfrom=@lavitalonandspa.com;
dmarc=NULL(p=NULL sp=NULL dis=NULL) header.from=suntitle.com;
Received-SPF: fail (domain of lavitalonandspa.com does not designate 173.201.193.36 as permitted sender)
X-YMailISG: KC7z7r4WLDthXswQevbwTODCGOf6cyX3NxmT_dp9PKuYRNJ.
3aCVuBU0wbQt4GpAChPZudNBP.rFBhwBUV5qZU7dKkpJy3d4Kt1E_9oQeVRS
uHy0SP3Ut1XfmDSGjf9ASpjBUYGEfUsUNKHdn0lF8Y52hDzy95uxocC4aDIN
eZpfbreSYPeSplVloyAV6LRPwgmNY_0Vvk8DHPo2UrHfUmbcDuxgD34MQAqdp
r4UipFAMrWzX74D_EEcT4hFbinNy8.9qTH8YY9vHpmRXo14dz1sPvd1JNdy7
wCw1RHT6J1TVHNjwqSbRTYNLA1wtD8za0IqJi8mV9iXKSlyk_Zia_2CBw1Jf
y36VB41f9HEUJHfvrbStyw1V_J.aOOEqHR3TenbX1aeFXHwdD9tAeX51d8p8
DDQOjGw2J18NG_aEvHHnt4rtZsYftgQsXlP5Lhkjw7JLRomXhvRCBHXt4PF
juNMDQg9x6A9ZD2u8pnmCnFvL.AJb3jTOMgX38_oe_1HqM0_KdIH3wbd9Qh2
EmsEHhuN0PT7C5aUGj8fzSip2Lz4eCE7mJFLO6mFwb.sTZp8v0w1_E2Y4jyb6
cWV4SwqBTyexmw679GqRXPgD4o016netpFJ3ES8a13wg_8uG1j1d4516TZB1
cKk4rdgFIsQuABedtnjM9jwr19r6YHWNpsV5PdGpuWJIH2r4q0j.XbJ3gqjQ
jQguRs_0cpjFHJoRyNueQl.wbqPZtT8R6xQwI3R0qaQ.dwfqiXZj87eK8jf
hgZWT9XxaPfs_onM4hBNeIcu_QiM0Pj1QvAXyb9vZuOZ0miHJ8ZE3mV8D
NGfUCJxd2bbZd2YOWg00P000cwIup5kCYShXLRJ2d7s2rgBXxYHC5Ljw.Er0
Fb_CrChyk1nNa68A0BAitdvaevAdHoUAc1UGPKXTEMQEJcFgapoAxCMy3D3x
BY3lgJ330Khx8p2ALPt9y3_WZ1_8LfLvnaw2q3xpUICFjZKr5iNkDzaVy0Tx
qZvyPPoB1j1v7WQYDM6G7GkpZqNEAFU32AxNkFhLmAe3wc8UGpbmyMRch3at
th0X58fybo79cKEHhtgtngBpbsb0C7kvaOumFGpLp1INKGAIJe9114MaVJXg
yAi2dGwdx4qqf3gnZmn1cJjFeHRKtT2Jd2LKx7bq2R_1hPQKBtv4FrQdD.or
uEcNhKwzDHC29x_DNuStf87TELSmfTdlK8IpiuI-
X-Originating-IP: [173.201.193.36]
Received: from 10.197.41.12 (EHLO p3plwbeout15-02.prod.phx3.secureserver.net) (173.201.193.36)
by mta4196.mail.bf1.yahoo.com with SMTPS; Mon, 25 May 2020 14:00:35 +0000
Received: from p3plgemwbe15-03.prod.phx3.secureserver.net ([173.201.193.9])
```



# Fraud 1: Spoofed Identity

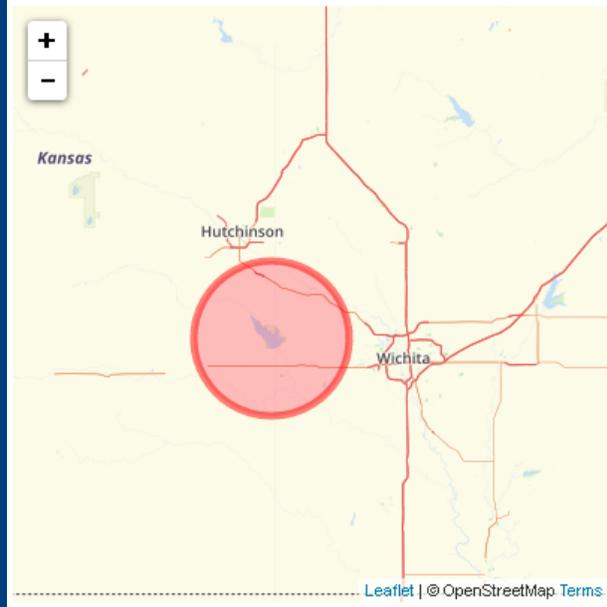
Continent: North America

Country: United States 

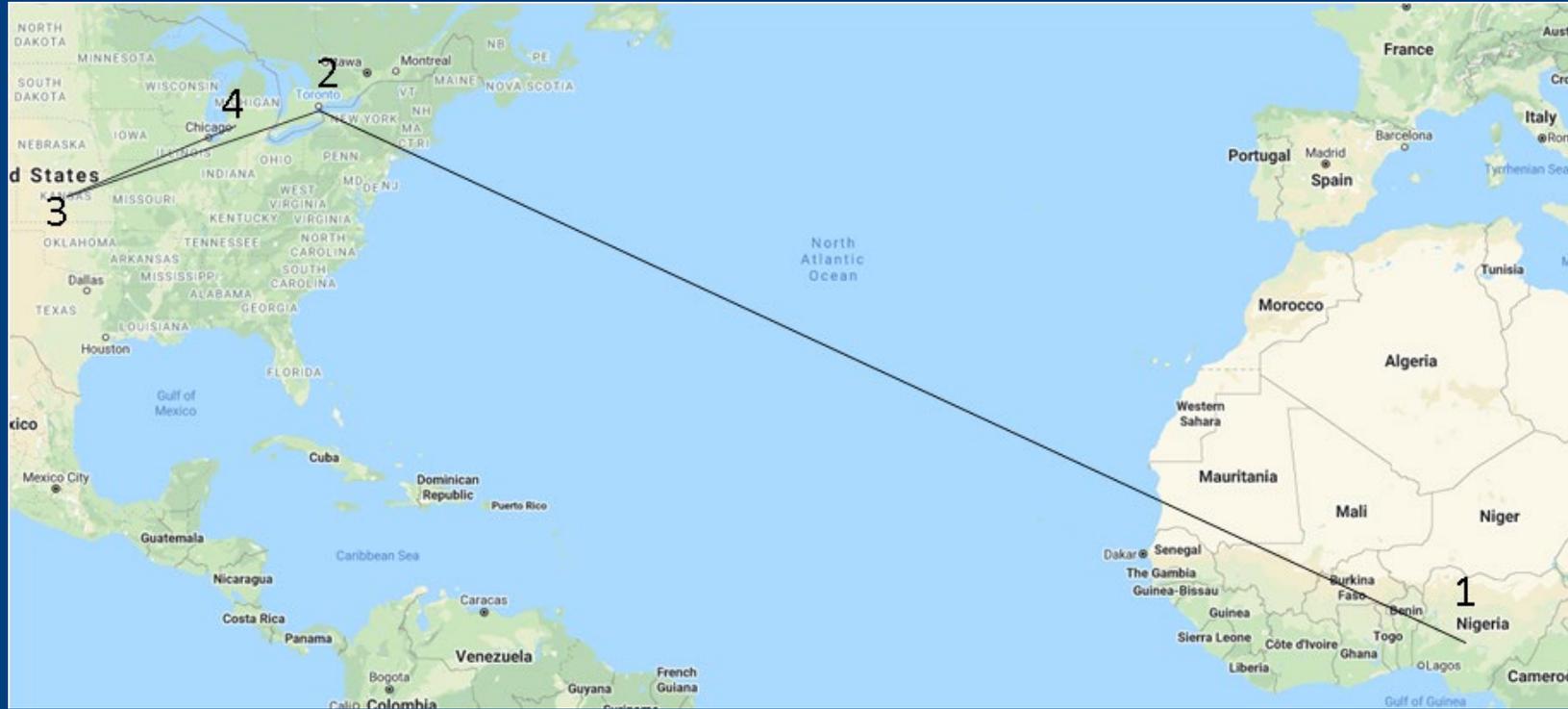
Latitude: 37.751 (37° 45' 3.60" N)

Longitude: -97.822 (97° 49' 19.20" W)

## Geolocation Map



# Fraud 1: Spoofed Identity



# Fraud 2: Mortgage Payoff Wire

## Parties Involved



Private Lender



Escrow Officer



Spoofed Private lender



# Fraud 2: Mortgage Payoff Wire

## Activity



Private Lender: Email is compromised and fraudster monitors traffic from title company's closer and private lender.



Spoofed Private Lender: Sends fraudulent payoff to closer.



Escrow Closer: Calls to verify wire instructions and sends wire to fraudulent account.



# Fraud 2: Mortgage Payoff Wire

May 21, 2020

*Fraudulent wire instructions*

[Redacted]

To Whom It Concerns:

This letter serves as notice of payoff amount for the loan on the above referenced property.

The payoff for the referenced property is \$ [Redacted]. This payoff is valid through May 28, 2020.

The borrower is [Redacted]. Following is the information required for wire transfer:

[Redacted]

Financial Institution: BoA  
Bank address: 222 Broadway  
New York, NY 10038

Business Checking Account NO. [Redacted]  
Routing No. [Redacted]  
Amount: \$ [Redacted]

Please prepare the cancellation deed for me, you may email me and I will get it signed and notarized once the payoff is received. You may charge the fee to the borrower

*fee charge*

Thank you,

[Redacted]



**Result: +\$130,000 was wired  
on Friday, May 22, 2020**



# Fraud 2: Seller net proceeds wire



## Money Muling

Account name on wiring instructions “not even close” to the account name on the fraudulent account

5/22 – money transferred to fraudulent account

5/26 – 1/3 of funds remaining in account

5/26 – 2/3 of funds were sent to US Bank via wire transfer

5/26 – two cashier’s checks were “immediately” prepared out of US Bank account for entire 2/3 amount

5/27 – one cashier’s check cleared

5/27 – fraud recovery initiated

5/28 – the second cashier’s check was “held” at a 3rd bank

5/28 – court order being requested to keep second cashier’s check held



# Today's Topics

- The Growth of Wire Fraud and COVID Scams
- Recent Fraud Examples
- **Money Laundering and Wire Fraud Recovery**
- Five Key Take-Aways



# Poll Question #3



# Money Muling and Wire Fraud Recovery

## Hour 1

- Initiate a “SWIFT” recall notice
  - Notify your bank
  - Initiate a “SWIFT” recall
  - Demand that funds are “frozen”
  - Confirm the location of subsequent transfers



# Money Muling and Wire Fraud Recovery

## Hour 1

### ○ Initiate a “SWIFT” recall notice

- Notify your bank;
- Initiate a “SWIFT” recall;
- Demand that funds are “frozen”; and
- Confirm the location of subsequent transfers

### ● File a complaint with the FBI

- Go to <https://www.ic3.gov/complaint/default.aspx/> to file a complaint with IC3 ([www.IC3.com](http://www.IC3.com)) and be prepared to provide the following information:
  - Victim’s name, address, telephone, and email;
  - Financial transaction information (e.g., account information, transaction date and amount, who received the money);
  - Under the Financial Transaction(s) section of the form, select “Wire Transfer” from the Transaction Type drop down menu.
  - Subject’s name, address, telephone, email, website, and IP address;
  - Specific details on how you were victimized;
  - Email header(s); and
  - Any other relevant information you believe is necessary to support y our complaint.
- Note and retain your IC3 Complaint Number – you will need to give that to the FBI field office (see below).



# IC3 Report



## Complaint Referral Form Internet Crime Complaint Center

Based on the information you provided it appears you may be the victim of fraudulent financial activity. As soon as possible, please contact your bank to send a Hold Harmless Letter or Letter of Indemnity (LOI) to the 'Recipient Bank'. Due to the time-sensitive nature of crimes involving fraudulent wire transactions, your bank should initiate a recall of funds as soon as possible.

**Thank you for submitting your complaint to the IC3. Please save or print a copy for your records. *This is the only time you will have to make a copy of your complaint.***

### Victim Information

Name: [REDACTED]  
Are you reporting on behalf of a business? No  
Business Name:  
Is the incident currently impacting business [None]  
operations?  
Age: Over 60  
Address: [REDACTED]  
Address (continued):  
Suite/Apt./Mail Stop:  
City: Grand Rapids  
County: Kent  
Country: United States of America  
State: Michigan  
Zip Code/Route: 49508  
Phone Number: [REDACTED]  
Email Address: [REDACTED]@gmail.com  
Business IT POC, if applicable:  
Other Business POC, if applicable:



# IC3 Report

## Financial Transaction(s)

Transaction Type: Wire Transfer

If other, please specify:

Transaction Amount: \$55000

Transaction Date: 05/22/2020

Was the money sent? Yes

Victim Bank Name: Chase Bank  
Victim Bank Address: 9235 Cherry Valley Avenue SE  
Victim Bank Address (continued): Caledonia  
Victim Bank Suite/Mail Stop: 49316  
Victim Bank City: Caledonia  
Victim Bank Country: United States of America  
Victim Bank State Michigan  
Victim Bank Zip Code/Route: 49316  
Victim Name on Account: Chase Bank  
Victim Account Number: [REDACTED]

Recipient Bank Name: Chase Bank  
Recipient Bank Address: 570 Broad St  
Recipient Bank Address (continued): Ste 110  
Recipient Bank Suite/Mail Stop: 07102  
Recipient Bank City: Newark  
Recipient Bank Country: United States of America  
Recipient Bank State New Jersey  
Recipient Bank Zip Code/Route: 07102  
Recipient Name on Account: Sun Title Agency  
Recipient Bank Routing Number: 021000021  
Recipient Account Number: 612866282  
Recipient Bank SWIFT Code:



# IC3 Report

## Description of Incident

Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.

I am in the process of closing on a commercial property located at 725 36th Street, SW, Wyoming, MI 49509. As part of the real estate closing, I received an email from my commercial broker with wiring instructions attached. I wired \$55,000 from my Chase Bank account in Caledonia, MI to a Chase Bank account in Newark, NJ as instructed in the wiring instructions. I learned today that the instructions were fraudulent and the information appears to have come from an email address intended to spoof the identity of the escrow officer of the company handling the closing.

Which of the following were used in this incident? (Check all that apply.)

- Spoofed Email
- Similar Domain
- Email Intrusion
- Other Please specify:

*Law enforcement or regulatory agencies may desire copies of pertinent documents or other evidence regarding your complaint.*

*Originals should be retained for use by law enforcement agencies.*



# IC3 Report

## Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

From: Renee M VanDriel <rvandriel@suntitle.com>

To: [REDACTED]@yahoo.com>

Sent: Wednesday, May 20, 2020, 8:08:17 AM EDT

Subject: 725 36th St.

[REDACTED]

Attached you will find a copy of the Final Hud for your Approval and our wire instructions for buyers funding towards closing also kindly advise buyer to make payment before closing date and send a receipt so we can get all arranged for a quick closing on the 27th. Please review and let me know of any changes thank you.

Thank you



# IC3 Report

Renee VanDriel  
Commercial Escrow Officer  
Sun Title Agency  
1410 Plainfield Ave., N.E.  
Grand Rapids, MI 49506  
(616) 458-9111 x2470 Main Line  
(616) 458-9302 Fax  
[www.suntitle.com](http://www.suntitle.com)

CORONAVIRUS NOTICE: If you are scheduled for a closing or plan to visit one of our offices, please postpone or reschedule your visit if you have any symptoms which may be similar to Coronavirus (fever, cough, shortness of breath, etc.) or have been in close proximity to someone who has these symptoms. We have alternative arrangements we can use for signing and delivering documents. Here is a link to our current protocols relating to Coronavirus: [www.suntitle.com/coronavirus](http://www.suntitle.com/coronavirus)

\*\*\*WIRE FRAUD ALERT\*\*\* We only deliver our wiring instructions to buyers and sellers through CertifID, an identity verification and bank account confirmation system ([www.certifid.com](http://www.certifid.com)). If you are a buyer or seller, you should NEVER accept wiring instructions from any other source or any other party to the transaction. Our wiring instructions never change – if you receive “new” wiring instructions, DO NOT USE THEM, and contact our office immediately using the phone number on our website. Everyone should protect themselves by verifying any wiring instructions via CertifID (or similar methods) or using a telephone number that is independently verified from a source other than the proposed wiring instructions.

The information contained in the preceding message is intended for viewing by the named addressee(s) only. This transmission may contain information that is privileged or otherwise confidential and is not intended for transmission to, or receipt by, anyone other than the named addressee(s). This transmission should not be copied or forwarded to anyone other than the named addressee(s). If you have received this transmission in error, please destroy and delete it from your system without copying or forwarding it, and notify the sender of the error by calling the phone number listed above.

From: Renee Vandriel [mailto:[rvandriel11@yahoo.com](mailto:rvandriel11@yahoo.com)]  
Sent: Tuesday, May 19, 2020 12:54 PM  
To: Renee M. VanDriel  
Subject: Fwd: Scanned document from HP ePrint user



# IC3 Report

\*\*EXTERNAL EMAIL\*\*

Sent from my iPhone

Begin forwarded message:

From: eprintcenter@hp8.us  
Date: May 19, 2020 at 12:50:39 PM EDT  
To: RVandriel11@yahoo.com  
Subject: Scanned document from HP ePrint user

This email and attachment are sent on behalf of rvandriel11@yahoo.com.

If you do not want to receive this email in future, you may contact rvandriel11@yahoo.com directly or you may consult your email application for spam or junk email filtering options.

Regards,  
HP Team

Are there any other witnesses or victims to this incident?

██████████ and Tom Cronkright

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

[No response provided]

Check here if this an update to a previously filed complaint:



# IC3 Report

## Who Filed the Complaint

Were you the victim in the incident described above? Yes

## Digital Signature

By digitally signing this document, I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S. Code, Section 1001)

Digital Signature: [REDACTED]

Thank you for submitting your complaint to the IC3. Please save or print a copy for your records. ***This is the only time you will have to make a copy of your complaint.***



## Hour 2

Contact your local FBI field office

- Find the FBI office nearest you (<https://www.fbi.gov/contact-us/field-offices>);
- Contact the Special Agent for cyber crimes;
- Give the SA the IC3 complaint number and other facts;
- Share contact info with the SA; and
- Align expectations.



## Hour 2

### Contact your local FBI field office

- Find the FBI office nearest you (<https://www.fbi.gov/contact-us/field-offices>);
- Contact the Special Agent for cyber crimes;
- Give the SA the IC3 complaint number and other facts;
- Share contact info with the SA; and
- Align expectations.

### Contact legal counsel

- File an action to obtain an injunctive order?
- Serve the injunctive order on all banks?



## Hour 3

### Contact all banks in the chain

- Contact the fraud prevention desk of the receiving bank;
- Help them identify the fraudulent transfer;
- Initiate the “SWIFT” recall notice and confirm funds have been frozen;
- Obtain the names of other banks that received your funds;
- Share contact information; and
- Align expectations.



## Hour 3

### Contact all banks in the chain

- Find the FBI office nearest you (<https://www.fbi.gov/contact-us/field-offices>);
- Contact the Special Agent for cyber crimes;
- Give the SA the IC3 complaint number and other facts;
- Share contact info with the SA; and
- Align expectations.

### Notify your insurance carrier

- If you hold errors and omissions coverage, professional liability coverage or any form of cyber security or cyber loss coverage, contact your insurance agent and place your insurer on notice of the incident.



## Hour 4

### Contact local authorities

- Call the local authorities and file a police report;
- Provide local authorities with all relevant information;
- Obtain and save the incident or report number;
- Share contact; and
- Align expectations



## Hour 4

### Contact local authorities

- Find the FBI office nearest you (<https://www.fbi.gov/contact-us/field-offices>);
- Contact the Special Agent for cyber crimes;
- Give the SA the IC3 complaint number and other facts;
- Share contact info with the SA; and
- Align expectations.

## Hour 5

### Contact your IT and security teams

- Initiate “The Information Technology Kill Chain”
- Determine the source of the breach;
- Contact your internal or external security/IT group before changing any settings or configurations on the environment;
- Contact you internal or external security/IT group to explain the situation and that a full “image” of the system needs to be created for eForensic purposes; and
- If warranted, eForensics investigators can be dispatched from a variety of sources to investigate the incident to determine if the data suggests greater impact on the environment.



# Main Takeaways



Details should come quickly, but the money may come back slowly.



Be prepared to “indemnify” the bank returning the funds.



Don't trust anyone proactively reaching out to you about your fraud.



# Today's Topics

- The Growth of Wire Fraud and COVID Scams
- Recent Fraud Examples
- Money Laundering and Wire Fraud Recovery
- **Five Key Takeaways**



# Key Takeaways

- Create a Culture of Compliance
- Educated and Engaged Employees
- Reduce Your Attack Surface
- Protect the Transfer of Money
- Adequately Insure the Risk



# Security Additional Best Practices

- Devise a continuity of operations plan for a potential cyber attack; prioritize the systems most important to continued operations.
- Use e-mail authentication protocols such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-Based Message Authentication Reporting and Conformance (DMARC), and Sender ID Framework (SIDF).
- Establish a training mechanism to inform end users on proper email and web usage, highlighting current information and analysis, and including common indicators of phishing. End users should have clear instructions on how to report unusual or suspicious emails.
- Regularly patch operating systems, software, and firmware.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Use multi-factor authentication where possible.
- Audit networks and systems for unauthorized remote communication.
- Disable or remove unneeded software, protocols, macros, and portals.



# How Can I Help?



[tcronkright@certifid.com](mailto:tcronkright@certifid.com)

## Tom Cronkright

- Co-Founder and CEO, CertifID
- Licensed Attorney
- Large Title Agency Owner
- Wire Fraud Victim
- National Speaker on Wire Fraud and Cyber Security

