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

Tom Cronkright

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

tcronkright@certifid.com
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

+96%  Of groups’ primary motivation is intelligence gathering

+400% Number of incoming reports about hacking

Source: PhishMe
Source: Symantec’s Internet Security Threat Report 2019
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.

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

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

Source: Proofpoint
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

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.
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%)
Spoofed Domain Registrations
Real Domain : hxxp://ripleys.com

Spoofed Domain : 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[@]foreslghtasg.com” via DomainTools

- Christywhite.com - Legitimate – christywhite.com
- Columbuszoo.org - Legitimate – columbuszoo.org
- Nciinc.com - Legitimate – nciinc.com
- Ripleys.com - Legitimate – ripleys.com
- Rockwellcollins.com - Legitimate – rockwellcollins.com
- Turkeyhill.com - Legitimate – turkeyhill.com

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Create Date</th>
<th>Registrar</th>
</tr>
</thead>
<tbody>
<tr>
<td>christywhite.com</td>
<td>2017-03-17</td>
<td>1&amp;1 INTERNET SE</td>
</tr>
<tr>
<td>columbuszoo.org</td>
<td>2017-03-17</td>
<td>SCHLUND DE</td>
</tr>
<tr>
<td>nciinc.com</td>
<td>2017-03-17</td>
<td>1&amp;1 INTERNET SE</td>
</tr>
<tr>
<td>ripleys.com</td>
<td>2017-03-17</td>
<td>1&amp;1 INTERNET SE</td>
</tr>
<tr>
<td>rockwellcollins.com</td>
<td>2017-03-17</td>
<td>1&amp;1 INTERNET SE</td>
</tr>
<tr>
<td>turkeyhill.com</td>
<td>2017-03-17</td>
<td>1&amp;1 INTERNET SE</td>
</tr>
</tbody>
</table>
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 “jjjmmoreinc9090@mail.com”

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Create Date</th>
<th>Registrar</th>
</tr>
</thead>
<tbody>
<tr>
<td>arttherapystudio.org</td>
<td>2017-03-15</td>
<td>--</td>
</tr>
<tr>
<td>atlanticairports.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>decks-docks.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>foresightasg.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>gemrc.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>iditrade.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>insrned.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>locicontrols.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
<tr>
<td>merittechcapital.com</td>
<td>2017-03-15</td>
<td>161 INTERNET SE</td>
</tr>
</tbody>
</table>
Initial Target (1)
ripleys.com -Legitimate – ripleys.com

Additional Targets (14)
christywhite.com -Legitimate – christywhite.com
columbuszoo.org -Legitimate – columbuszoo.org
nciiinc.com -Legitimate – nciiinc.com
ripleys.com -Legitimate – ripleys.com
rockwellcollins.com -Legitimate – rockwellcollins.com
turkeyhill.com -Legitimate – turkeyhill.com
arttherapystudio.org -Legitimate – arttherapystudio.org
atlanticaimports.com -Legitimate – atlanticaimports.com
decks-docks.com -Legitimate – decks-docks.com
foresightasg.com -Legitimate – foresightasg.com
gemrc.com -Legitimate – gemrc.com
iditrade.com -Legitimate – iditrade.com
insmed.com -Legitimate – insmed.com
locicontrols.com -Legitimate – locicontrols.com
meritechcapital.com -Legitimate – meritechcapital.com
NCI INC reported they received an email from a spoofed domain targeting one of their personnel from spoofed domain “@NCIIINC.COM”

Business specifically targeted - Suspects know who to send the email 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 St W, Wyoming, Mn. wants to know if the attached resolution meets your approval if signed. Thanks

[attaches document]

On May 15, 2020, at 9:05 AM, Renee VanDriel <rvaendriel@wj.com> wrote:

Good morning,

Yes, it looks acceptable.

Thanks

Renee VanDriel
GTC Title Agency
1037 Main Ave. N 120
Grand Forks, ND 58201

Phone: (701) 774-0500

Fax: (701) 774-0501

Email: rvaendriel@wj.com

[attaches document]

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

Sent from my iPhone
Fraud 1: Buyer Cash to Close

On Mon, May 10, 2020, 02:44:45 PM GMT+1, Manale M. VanDriel <manale@lecture.com> wrote:

The 3P works for me. What’s up?

Manale M. VanDriel
Compliance Officer
Bank Title Agency
1801 Pastora Street, 7FL
San Antonio, TX 78207
(210) 457-6363 Mobile
(210) 457-6362 Fax
www.banktitle.com

CORPORATE NOTICE: If you are served with a civil process to collect any of our fees, please promptly serve and return the original and any additional documents to our office. This notice shall not be construed as an offer of any additional services or any other services to the person who has served the process.

Automated PHONE ALERT: We will update your company’s credit reports and call you to confirm your credit instructions. If you are a buyer or seller, you should never accept unsolicited credit or any other service on any of your own funds without contacting us. We are unable to answer any questions on the phone or by email. Please contact us in writing for more information.

You will receive a confirmation number on our website. Everyone should contact themselves by verifying your information through CREDID or (similar method) as a security tool. If you are not sure if your credit information is outdated or incorrect, please contact us in writing for more information.

In the event of a fraudulent transaction involving your name or your account number or otherwise confirmed in an email or letter or over the phone, immediately contact your bank or credit card company and notify the credit card company of the fraud.

Good morning,

Kindly advise as the closing date for the 3rd two-way can be scheduled for closing this month.

Please VanDriel
Compliance Officer
Bank Title Agency
1801 Pastora Street, 7FL
San Antonio, TX 78207
(210) 457-6363 Mobile
(210) 457-6362 Fax
www.banktitle.com

CORPORATE NOTICE: If you are served with a civil process to collect any of our fees, please promptly serve and return the original and any additional documents to our office. This notice shall not be construed as an offer of any additional services or any other services to the person who has served the process.
Fraud 1: Buyer Cash to Close

----- Forwarded Message -----
From: Renee M VanDriel <rvandriell@suntitle.com>
To: 
Sent: Wednesday, May 20, 2020, 8:08:17 AM EDT
Subject: 

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 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 Main Line
(616) 458-9302 Fax
www.sunitle.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
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.
Fraud 1: Buyer Cash to Close

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

Thanks for the update. 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
Fraud 1: Buyer Cash to Close

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

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

Good Morning

Happy Memorial Day, We are closing on another property today and buyer already wired the purchase amount of $358,000 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

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
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
Fraud 1: Buyer Cash to Close

From: Donald
Sent: Monday, May 25, 2020 9:47 AM
To: Teresa M. Yazdi
Subject: Fwd: Buyer Statement - Fraud

--- Forwarded Message ---

From: Donald
Sent: Monday, May 25, 2020, 9:11 AM EDT
To: Teresa M. Yazdi

--- Forwarded Message ---

From: Teresa M. Yazdi
Sent: Monday, May 25, 2020, 9:11 AM EDT
Fraud 1: Buyer Cash to Close

----- Forwarded Message -----
From: Renee M VanDriel <rvandriel@suntitled.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
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
Fraud 1: Spoofed Identity
Fraud 1: Spoofed Identity
# Fraud 1: Spoofed Identity

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Header Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>@phishers.com, Mon, 25 May 2020 14:03:30 +0000</td>
</tr>
<tr>
<td>Return-Path</td>
<td><a href="mailto:.smtp@phishers.com">.smtp@phishers.com</a></td>
</tr>
<tr>
<td>Authentication-Path</td>
<td>xsmtp.com:1080, c=us, p=smtp, date=Mon, 25 May 2020 14:03:30 +0000, from=<a href="mailto:SMTP@phishers.com">SMTP@phishers.com</a>, server=xsmtp.com</td>
</tr>
<tr>
<td>Received</td>
<td>full: <a href="mailto:FAKE-SPAM@phishers.com">FAKE-SPAM@phishers.com</a>, date=17:29:57 25 May 2020, for=<a href="mailto:smtp@phishers.com">smtp@phishers.com</a></td>
</tr>
<tr>
<td>X-Originating-IP</td>
<td>171.201.394.30</td>
</tr>
<tr>
<td>X-SMTP-SERVER-ACCEPT</td>
<td><a href="mailto:6smtp@phishers.com">6smtp@phishers.com</a></td>
</tr>
<tr>
<td>From</td>
<td>&quot;Steve M. VanDriel&quot; <a href="mailto:sma@phishers.com">sma@phishers.com</a></td>
</tr>
<tr>
<td>X-Content</td>
<td><a href="mailto:6smtp@phishers.com">6smtp@phishers.com</a></td>
</tr>
<tr>
<td>Reply-To</td>
<td>&quot;Steve M. VanDriel&quot; <a href="mailto:sma@phishers.com">sma@phishers.com</a></td>
</tr>
<tr>
<td>Tmp</td>
<td>&quot;default&quot;<a href="mailto:sma@phishers.com">sma@phishers.com</a></td>
</tr>
<tr>
<td>Subject</td>
<td>Re: Steve’s statement</td>
</tr>
<tr>
<td>Date</td>
<td>Mon, 25 May 2020 07:00:01 +0000</td>
</tr>
<tr>
<td>Mime-Version</td>
<td>1.0</td>
</tr>
<tr>
<td>X-Translator-Name</td>
<td>From: phishers.com To: Steve VanDriel@<a href="mailto:sma@gmail.com">sma@gmail.com</a></td>
</tr>
</tbody>
</table>
Fraud 1: Spoofed Identity
Fraud 1: Spoofed Identity

Geolocation Map

- Continent: North America
  - Country: United States
  - Latitude: 37.751 (37° 45' 38" N)
  - Longitude: -97.822 (97° 49' 18.2" W)
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

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 $500,000.00. This payoff is valid through May 25, 2020.

The borrower is: [redacted]

[redacted]

In the event that a wire transfer is required, the following information is needed:

Financial Institution: [redacted]
Bank Address: 222 Broadway
New York, NY 10013

Transaction Number: [redacted]
Routing No: [redacted]
Account No: [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.

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

- 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) 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 your 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: [Redacted]
Is the incident currently impacting business [None]
operations? Over 60
Age: [Redacted]
Address: [Redacted]
Address (continued):
Suite/Apt./Mail Stop: [Redacted]
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: [Redacted]
Other Business POC, if applicable: [Redacted]
<table>
<thead>
<tr>
<th>Financial Transaction(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction Type:</strong> Wire Transfer</td>
</tr>
<tr>
<td>If other, please specify:</td>
</tr>
<tr>
<td><strong>Transaction Amount:</strong> $55000</td>
</tr>
<tr>
<td><strong>Transaction Date:</strong> 05/22/2020</td>
</tr>
<tr>
<td><strong>Was the money sent? Yes</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Victim Bank Name: Chase Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Victim Bank Address:</strong> 9235 Cherry Valley Avenue SE</td>
</tr>
<tr>
<td><strong>Victim Bank Address (continued):</strong> Caledonia</td>
</tr>
<tr>
<td><strong>Victim Bank Suite/Mail Stop:</strong> 49316</td>
</tr>
<tr>
<td><strong>Victim Bank City:</strong> Caledonia</td>
</tr>
<tr>
<td><strong>Victim Bank Country:</strong> United States of America</td>
</tr>
<tr>
<td><strong>Victim Bank State:</strong> Michigan</td>
</tr>
<tr>
<td><strong>Victim Bank Zip Code/Route:</strong> 49316</td>
</tr>
<tr>
<td><strong>Victim Name on Account:</strong> [Obfuscated]</td>
</tr>
<tr>
<td><strong>Victim Account Number:</strong> [Obfuscated]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recipient Bank Name: Chase Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recipient Bank Address:</strong> 570 Broad St</td>
</tr>
<tr>
<td><strong>Recipient Bank Address (continued):</strong> Ste 110</td>
</tr>
<tr>
<td><strong>Recipient Bank Suite/Mail Stop:</strong> 07102</td>
</tr>
<tr>
<td><strong>Recipient Bank City:</strong> Newark</td>
</tr>
<tr>
<td><strong>Recipient Bank Country:</strong> United States of America</td>
</tr>
<tr>
<td><strong>Recipient Bank State:</strong> New Jersey</td>
</tr>
<tr>
<td><strong>Recipient Bank Zip Code/Route:</strong> 07102</td>
</tr>
<tr>
<td><strong>Recipient Name on Account:</strong> Sun Title Agency</td>
</tr>
<tr>
<td><strong>Recipient Bank Routing Number:</strong> 021000021</td>
</tr>
<tr>
<td><strong>Recipient Account Number:</strong> 612866262</td>
</tr>
<tr>
<td><strong>Recipient Bank SWIFT Code:</strong></td>
</tr>
</tbody>
</table>
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.
If an email was used in this incident, please provide a copy of the entire email including full email headers.

From: Renee M VanDrie <rvandrie@suntile.com>

To: [Redacted]@yahoocom

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
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

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

***WIRE FRAUD ALERT*** We only deliver our wiring instructions to buyers and sellers through Certified, an identity verification and bank account confirmation system (www.certified.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 Certified (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:rsvandriel11@yahoo.com]
Sent: Tuesday, May 19, 2020 12:34 PM
To: Renee M. VanDriel
Subject: Fwd: Scanned document from HP ePrint user
**EXTERNAL EMAIL**

Sent from my iPhone

Begin forwarded message:

From: eprintcenter@hp8.us  
Date: May 19, 2020 at 12:50:30 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: **********

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 your 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?

Tom Cronkright

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

tcronkright@certifid.com