Cybersecurity and Fraud in the COVID-19 Environment

April 29, 2020

Heather Staverman

Director of Meetings and Exhibits

Equipment Leasing and Finance Association

Today's Speakers

Tom Ware
President
Tom Ware Advisory Services, LLC

Dominic Liberatore
Deputy General Counsel
DLL

Andrew Cotter
EVP, Chief Information Officer
Somerset Capital Group, Ltd.

Tom Ware

President

Tom Ware Advisory Services, LLC

Leasing Fraud in a COVID-19 World

- Every action requires both desire and ability, and both the desire and ability of fraudsters has increased on the past couple months.

- "Fraud" is a spectrum:

  - "**Total Fraud**" is attempted theft, never once intending to repay. Can be by obligors and/or intermediaries.

  - "**Partial Fraud**" is lying to entice a lender to approve a transaction that probably wouldn't if they knew the full truth. The obligor intends to repay (if they can) but the risk is very high.

  - "**Technical Fraud**" (which some might not consider fraud at all) occurs in documentation, when for example one person signs for another, or says equipment has all been delivered, when it hasn't. It is motivated by convenience and expediency, without anyone realizing they are doing any harm.

“Total Fraud”

- With so many people unemployed and business shuttered, there is a lot more motivation.
- The classic fraudster trick of pretending to be an established business (borrower or dealer) that they are not, will be easier with people working from home and businesses temporarily closed.
- In the consumer space, there are fraudsters who establish hundreds of fictious identities, run all their financial lives for a couple years, making auto payments etc., and then max out all their credit and “harvest” them all before then disappearing.
- In the commercial equipment finance world, the equivalent is the “pump and dump,” when a borrower does 2-3-4 deals in a row and then disappears.
- Equipment finance lenders are reporting cases of synthetic websites, spoof e-mails and phone numbers, and e-mails being hacked to send fraudulent payment instructions to the lender.

"Total Fraud" *(con't)*

- Temporarily reduce automation.
- Pull more reports from PayNet, Lexis-Nexis, Secretaries of State, and other information providers.
- Use Google Earth, Satellite View and Street View.
- Online/digital verifications for phone numbers, addresses, etc.
- Funding not the place to make credit decisions, but a good place to catch many types of frauds.
- For transactions with less information – get first payment in advance – with a corporate check.
- Track the magnitude of fraud at the portfolio level; FPDs are a good proxy.
- Carefully monitor portfolio performance of vendors and other deal sources over time.

“Partial Fraud”

- Historically not as much of a problem as Total Frauds – but huge temptation today to pretend to finance equipment to get cash (and equipment inspections difficult now).
- Cash-strapped vendors and brokers will be tempted to collude (or suggest).
- Ask the otherwise unusual question “why would you want additional equipment now?”
- Classic true story is of a credit application by a day care center on the border of Mexico – for a backhoe. What do you think they are going to do with that?
- Equipment that is not common for the borrower’s type of business is a red flag, as is substantial geographic distance between a vendor and a borrower, without a logical reason – many times these are straw purchases for a friend or relative.
- Financing or pledging the same asset multiple times, often simultaneously, is common with both Partial Fraud and Total Fraud.

"Partial Fraud" *(con't)*

- Painting a rosier picture for the lender obviously improves the chance of approval.
- Alternative lenders got burned in 2013 approving loans based on doctored bank statements.
- Now get bank statements directly from the bank through a service like Yodlee (might also mitigate risk of fraudulent identity).
- Take extra care in examining equipment descriptions, ages, used equipment represented as new, and the reasonableness of the equipment values listed in vendors' invoices
- True Pic - an app to perform secure virtual equipment inspections.
- Differentiate due diligence by industry and/or asset type – e.g. IT equipment is inherently fertile territory for fraudsters, with subjective values and hard to verify capabilities.
- Look more closely at any requests from restaurants, brick-and-mortar retailers, hotels, energy producers, and other hard-hit industries.
- Requiring more personal guarantees might dissuade some Partial Fraudsters.

“Technical Fraud”

- “Technical Fraud” (which some people might not consider fraud) occurs when people sign documents for their co-workers, or most of the cases where the lessee says that all the equipment has been delivered, but it really hasn’t.
- Not pre-meditated or intended to gain an unfair advantage, but rather is generally motivated by expediency or laziness, not realizing this could cause a real problem later.
- Likely to increase – but for a completely different reason – the fact that very few professionals are co-located now, with most people working from home.
- Use Docusign or other electronic document systems and require copies of drivers’ licenses.
- Gather information on corporate officers’ home addresses, home phones, cell phones, etc., even if they are not guarantors (though admittedly this is not easy to do).

General Fraud Prevention

- Increasing fraud prevention requires extra time and work.
- Risk that important communication will be lost with people working from home.
- Culture of over-communication to overcome personal silos, esp. about anything that smells odd.
- Microsoft Teams can effectively foster better communication within departments.
- Single person review the vendor, collateral, credit, and documentation – to get a holistic view.
- Lenders should demand stronger protective processes and transaction terms today.
- For a more comprehensive list of red flags to watch out for: https://www.monitordaily.com/article-posts/preventing-equipment-fraud/
- Bill Verhelle, QuickFi CEO: future of fraud prevention is “secure mobile platforms with enhanced security capabilities – facial recognition, drivers license authentication, geo-location, device ID, two-factor text and company e-mail authentications.”

Dominic Liberatore

Deputy General Counsel

DLL

Fraud in the Digital World

- Fraud in the digital world can arise through email correspondence and attachments, e-signed leases or full-blown e-leases. Sometimes a funder will face “old school” deception. Increasingly funders are facing higher tech fraud that is more difficult to detect. Goal of this session is to highlight some practical tips to combat fraud in the modern world.
- One common type of fraud in digital world is email fraud. As the old adage goes, **to be forewarned is to be forearmed**. Some examples include:
    - **phishing** (often confused with spoofing – someone attempts to steal financial or confidential information by pretending to be a legitimate person,
    - **spoofing** – a person impersonates another user or device in order to launch some form of fraud or network attack, and
    - **phony emails with phony links** – links that take the user to the fraudster’s website rather than a legitimate site).

Fraud in the Digital World

- Paperless equipment finance transactions (e-signing & e-leases) more commonplace in last few years. ELFA led an outreach a few years ago and committed fair amount of time and focus. Further, as a result of COVID19, many ELFA members working remotely during pandemic. This means more e-signing and e-leasing. This trend will only continue.

- This increase of paperless transaction is a good thing. However, creates opportunities for bad actors since virtually all face to face interactions replaced by electronic ones. Consider what a big change this is from just 5 or 10 years ago.

- Distinction between e-signing and full-blown e-leases.

- Done properly, e-signing and e-leasing just as secure as (potentially more than) paper leases. However, easy to get complacent in digital world. It's imperative not to do so. Follow your process and follow the basics.

Practical Recommendations for Combatting Fraud in the Digital World

- To minimize fraud risk for equipment finance transactions, consider:
  - Which e-sign provider will be used, one selected by the funder or instead by customer? If selected by you, you will have already performed your due diligence on the provider for signer authentication process (many providers offer different levels of signer authentication), size and overall viability, platform and security protections, audit trail and e-vaulting capabilities (if applicable). Many providers out there. Not all are equal or industry known/accepted.
  - Is e-sign provider a recognized name in the market or a new and/or unknown entity? This is important for e-signing and crucial for securitizing and syndicating of full-blown e-leases.
  - Is e-sign service being done by customer itself (i.e., a "home grown" e-sign solution)? Same considerations as above. Heightened concern as to signer authentication. Think about this--how would you know who really signed for a home-grown solution? Raises some of the same concerns as signature stamp.
- All these questions go to strength and completeness of underlying processes and protections of e-sign service being used and, ultimately, enforceability of underlying leases.

Practical Recommendations for Combatting Fraud in the Digital World

- For equipment finance transactions, important to retain audit trail (certificate of completion). Not simply akin to cover sheet. This is a key document that summarizes who signed lease, date and time when signing occurred, and IP address(es) used.
- Whose e-sign *account* is to be used? Even if e-sign provider is same source used by funder (for instance, customer's or originating vendor's account), different signer authentication levels may have been chosen by e-sign account owner, or in the case of electronic leases, "single authoritative copy" process may not have been selected (for purpose of establishing who has sole "original").
  - If using e-sign account owned by entity other than funder, probably won't have ability to ask for audit trail directly from provider if not given to you by account owner.
- Signer Authentication. Does e-sign provider offer two-step verification, such as a text with a code, or some out of wallet identity check service? Some funders simply rely on using known email addresses. May be appropriate in a small ticket environment. However, given no face to face interactions, taking extra step is important and incremental time and cost generally not significant. Of course, need to balance with customer experience. Consider using different levels depending on dollar size.

Practical Recommendations for Combatting Fraud in the Digital World

- Similar to traditional fraud, in digital world crucial to remember and apply basics.
  - Due diligence on customer and its email address important.
  - Don't skip steps. Look at customer's email address closely.
  - If anything looks suspicious (and even if it doesn't!), hover cursor over email address(es) and any embedded links BEFORE clicking.
- Be on lookout for emails not from actual company email domain (John.DoeatABC@aol.com vs. John.Doe@ABC.com). Also, be wary of personal email addresses.
- Ask yourself, does email look "fishy", include typos or just seem off somehow (if so, dig deeper!).
- Funders need to train employees on basic technology issues, including email security precautions, IP addresses, URLs/website addresses, secured site designation, internet links and internet names.
- Trainings need to be followed by regular training refreshers and updates because technology and fraud techniques constantly changing.

Practical Recommendations for Combatting Fraud in the Digital World

- To minimize fraud risk, whether dealing with email correspondence and attachments, old fashioned wet ink signed paper leases or e-signed or full-blown e-leases, institute standard back office processes including required lessee due diligence and consistently apply, even for repeat business.
- Remember that common sense and due care needed just as much in digital world as paper world.
- Fraud is a constantly evolving threat. If some component of deal does not feel right, it might not be.
- Drill down, pick up phone, go to customer or perform other due diligence in light of facts and circumstances.
- It's always obvious…in hindsight!

Andrew Cotter

EVP, Chief Information Officer

Somerset Capital Group, Ltd.

Cybersecurity: Today's New Reality

- Shift to Work from Home
- Traditional planning cycles out the window
- Business continuity with no defined timeline
- Conditions that changed daily

"42% of U.S. workers who did not telecommute previously are doing so now"

CNBC All America Survey April 9th, 2020

Security has never been more important

Cybersecurity: Common Obstacles

Barriers making this challenge difficult to address

- IT scrambled to enable access and source equipment
- Employees unfamiliar with working from home
- Too much security restricts productivity
- Too little security opens the organization up to risk
- Existing plans were insufficient to maintain a viable security posture for such a large shift this quickly

“WHO reports fivefold increase in cyber attacks”

who.int 23 April 2020

Cybersecurity: Key Attack Vectors

- Phishing
- Insecure endpoints
- Malicious applications
- Zero Day Exploits
- Malware
- Malicious Insiders
- Trust relationships
- Unpatched vulnerabilities
- Ransomware
- Man-in-the-middle attack
- Weak and stolen credentials
- Advanced Persistent Threats
- Denial of Service
- SQL injection
- Weak encryption
- Misconfigured devices

145
Average number of security breaches in 2019

+11%
Increase in security breaches since last year

67%
Increase in security breaches in the last five years

Ninth Annual Cost of Cybercrime Study
March 6, 2019 accenture.com

Cybersecurity: Phishing

Types of Phishing Attacks

- **Spear phishing** - Targets a specific individual or group of individuals
- **Smishing** - SMS messages instead of email
- **Vishing** - An attack conducted by telephone
- **Whaling** - Business email compromise (BEC) targets a high-profile victim
- **Cloning** - Copies a legitimate email from a trusted sender replacing a link or file
- **Angler Phishing** – Using social media to masquerade as a legitimate party

"When in Doubt: Hang Up, Look Up, & Call Back"

Brian Krebs - KrebsonSecurity.com

Cybersecurity: Phishing

Phishing Techniques

- **Pharming** - Redirects a user to a bogus website
- **Link Spoofing** - Making a malicious URL appear similar to an authentic URL
- **Domain Spoofing** - Substitutes a false URL to deceive users
- **Session Hijacking** - Stolen session ID to impersonate a legitimate user
- **Pharming** – Cache poising against domain name system (DNS)
- **Evil Twin** – A rouge Wi-Fi access point masquerading as a legitimate one

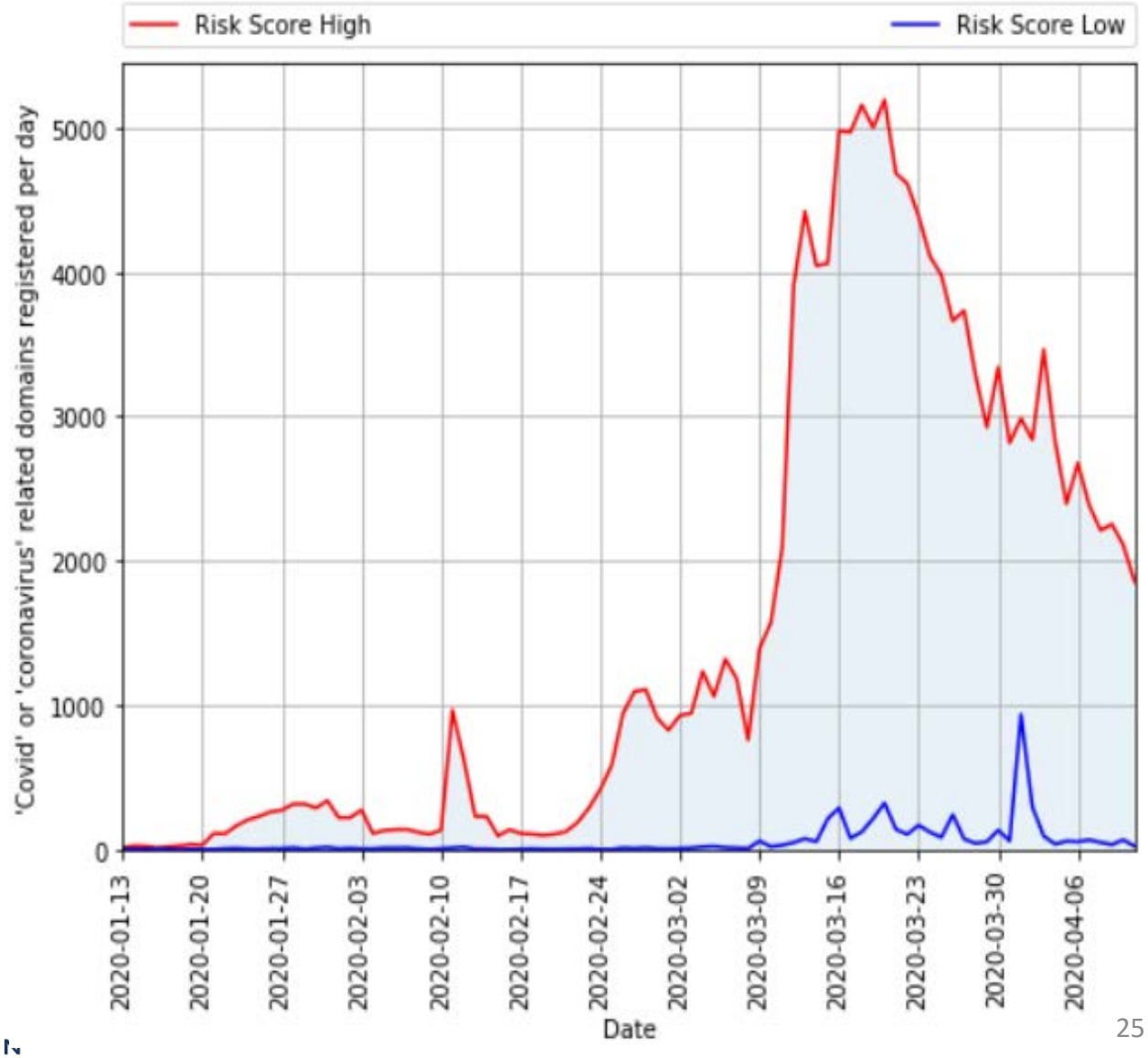
*"60% of Americans say they or a family member has been a **victim of a phishing attack**, and 15% will be targeted **more than once every year.*** Accenture study Jan 28, 2020

Cybersecurity: Phishing

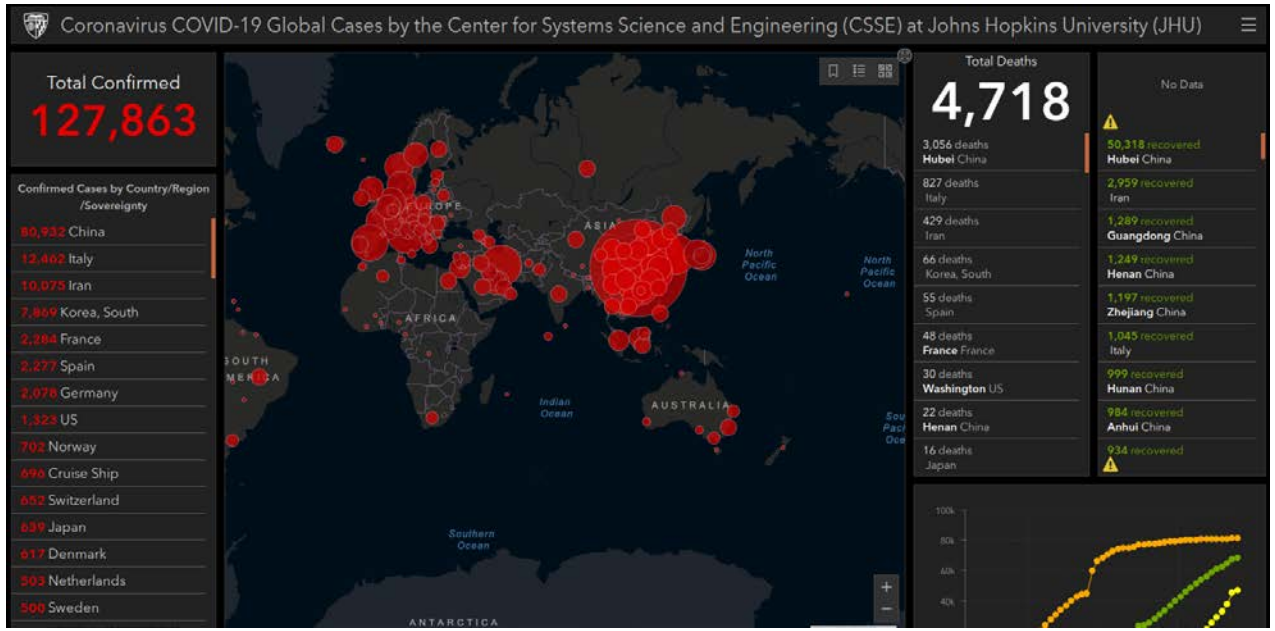
COVID-19 Related Domain Spoofing Activity

The total number of domains registered per day that contain a COVID-19 related term, according to DomainTools. The red line indicates the count of domains that DomainTools determined are "likely malicious." The blue line refers to domains that are likely benign.

~ KrebsonSecurity.com



Cybersecurity: Malware



Fake coronavirus live update style maps to spread the AzorUlt information stealing trojan

Investigation shows query traffic to a domain hosting a malicious COVID-19 map

April 1, 2020 umbrella.cisco.com

Cybersecurity: Ransomware

Ransomware attacks shot up 500% IN 2019.

Panda Security *2019: A Record-Breaking Year For Ransomware*

Ransomware-as-a-service (RaaS)

USD	BTC	Malware
$12.5M	~1,600	Ryuk
$10.9M	565	DoppelPaymer
$10.0M	1,326	REvil
$9.9M	1,250	Ryuk
$6.1M	850	Maze
$6.0M	763	REvil
$5.3M	680	Ryuk
$2.9M	375	DoppelPaymer
$2.5M	250	REvil
$2.5M	250	DoppelPaymer
$2.3M	300	Maze
$1.9M	250	DoppelPaymer
$1.6M	216	BitPaymer
$1.0M	128	Maze

Table 1.
Largest Ransom Demands Reported in 2019

Crowdstrike 2020 Global Threat Report

Cybersecurity: Advanced Persistent Threats

- Carefully planned and designed to infiltrate a specific organization
  - Infiltration
    - Gain access through an email, network, file or application vulnerability
  - Escalation and Lateral Movement
    - Attackers insert malware into an organization's network
    - They move laterally to map the network and gather credentials
  - Exfiltration
    - Typically store stolen information in a secure location within the network
    - They then extract, or "exfiltrate" it without detection.

Characteristics of an APT Attack: Unusual activity

Cybersecurity: LEIA

Leverage

- Start from your current processes
- Tailor them to accommodate the new way of remote working.

Evaluate

- Prioritize security items in a logical sequence
- Some security components may not be as time sensitive as others.

Implement

- Follow though on identified changes

Assess

- Monitor outcomes and emerging threats

Promotional photo of Fisher as Princess Leia for the original 1977 *Star Wars* film

Cybersecurity: Hygiene

Developed a culture of awareness

- Leveraged basic cybersecurity training
- Educate users about their responsibilities in a remote setting

Review your Business Continuity Plans

- Now is the time to update your runbooks

Expand monitoring

- Cyberattacks have proliferated
- Basic boundary-protection mechanisms won't secure users

Patch & Update Management

- Enable automatic updates whenever possible.
- Replace unsupported operating systems, applications and hardware.

External relationships

- Confirm the security of third parties.
- Sustain good procurement practices

Cybersecurity: Quick Wins

- Family members should not use your work computer
- Lock your computer when not in use
- Secure physical documents
- Required multifactor authentication (MFA)

10.9% of organizations' IT budgets is spent on cybersecurity programs

Accenture Study Jan 28, 2020

Your employees are your last line of defense