EQUIPMENT FINANCE ADVISOR
SERVING EQUIPMENT FINANCE DECISION MAKERS

Fighting Fraud in the Digital Age of Equipment Finance

By: John Beard and Dave English
Date: Aug 15, 2016 @ 07:00 AM

Digital technology is a great enabler. With it, equipment finance companies and those they serve can do more than they ever have, faster than they ever could and with greater reach than they've ever had. However, digital enables all of us equally, and that includes those out to defraud equipment finance companies and, by extension, the whole industry.

At its core, fraud hasn't changed. In the case of fraudulent equipment finance, the goal is primarily to steal identities – or create them out of thin air – in order to take delivery of equipment and then disappear with it or be paid for equipment and software that was only ever sold on paper, whether pulp or digital. The goals of thieves are the same as they ever were. But the means of achieving those goals now take advantage of digital tools and techniques.

Our response? The foundation of our fraud detection and prevention efforts is traditional and time tested, but it now also utilizes the process efficiencies offered by digital technology.

Thieves are always on the lookout for tools and techniques to support their goals. So are we.

But the perpetrators of fraud have an advantage that we haven't yet fully leveraged: *community.* Fraudsters aren't always lone wolves. Often, they're networked. They share. If one finds a vulnerability, peers know it almost instantly. And all it takes to be part of the club is a laptop and an internet connection.

The perpetrators of fraud are united against us. To fight them effectively, we need to work together too.

Fraud Never Sleeps

These 24/7 "would-be" thieves are sniffing and probing and looking for

chinks in the armor of our defenses. In some parts of the world, it's practically a national pastime.

Digital fraud has gone mainstream. Now, anyone with a little time, a modicum of effort and almost zero expertise can hack a password, breach a server, impersonate someone else, falsely resurrect a dead company or even create an entirely fictitious company, complete with fake credit reports and public records.

The tools to carry out these ambitions are absurdly easy to find and use. A simple Google search will get you started. From there, you'll quickly link down the rabbit hole where you'll find an embarrassment of riches: IP scanners, password hacking utilities, website vulnerability analyzers, phishing tools, message boards with helpful tips and tricks, even Dark Web hacking schools. And in keeping with the hacker ethos, it's all collaboratively updated and mostly free.

JOHN BEARD
SVP, Portfolio Quality
LEAF Commercial Capital, Inc.

Digital takes with one hand, but it gives with the other. Big Data is indispensable for originating, underwriting, documenting and funding transactions. That's even more true for small-ticket equipment finance, where efficiency can make or break a profit margin.

Digital fraud is all about the details, particularly the details someone else forgot ... the ones that give criminals a tiny crack they can pry apart and exploit. So we do our best to prevent those cracks in the first place. That means focusing our efforts on the earliest stages of the financing process: business sourcing and origination, focusing in particular on ensuring individuals and businesses are who and what they purport to be.

And like the hackers, phishers and fraudsters of all stripes, we need to collaborate to save time and money and increase the effectiveness and agility of our countermeasures. In that spirit, here are the basics of how our organization uses technology to detect and prevent equipment finance fraud, beginning with customer acquisition and authentication, continuing with underwriting and concluding with vendor funding, transaction completion and ongoing education.

Customer Acquisition and Authentication

LEAF invests heavily in equipment finance portals, secure system access Application Programmable Interfaces (APIs) and processes aimed at authenticating buyers and sellers across the finance workflow. But we've learned that our defense can be mounted even earlier, in the lead generation phase of our marketing efforts. Before we get into the work of gatekeeping, we decide where those gates should be placed and precisely who we'd like to attract to them.

We do that with a comprehensive behavior and persona targeting process designed to limit our brand exposure to our ideal customers. This "narrowcasting" approach not only gives us a baseline against which we can more easily detect and flag outliers, it allows us to better target our marketing and sales efforts. In addition, it communicates our awareness, like a porch light left on at night. It's a sign of welcome, but also of attention. Seeing that, thieves tend to seek easier, less-aware targets.

DAVE ENGLISH
EVP & Chief Investment Officer
LEAF Commercial Capital, Inc.

From there, we conduct an in-depth data recency/consistency analysis using a variety of databases and techniques, such as multifactor authentication. Are basics, including names, physical addresses, phone numbers and email addresses, consistent across databases and authentication channels? Is recently created information a necessary and truthful update or a fabrication? If there's no relatively recent data, is the business dormant or dead and being resuscitated only as a vehicle for equipment finance fraud?

Faced with these verification challenges, equipment finance companies often turn to the new breed of fintech service providers promising – but not always delivering – accurate and reliable customer verification. While these services can be helpful, they're not developed enough to be relied on solely.

Underwriting

In the underwriting stage of the process, the Five Cs of credit still apply. Credit management must carefully assess character, capacity, capital, collateral and conditions, albeit with updated digital tools, including consistency checks of customer demographic/firmographic data across multiple databases and services.

In addition to the standard reporting agencies, including Dun & Bradstreet, Equifax, Experian, PayNet and LexisNexis, social media can be an important

verification tool. Alternative databases, such as those maintained by DirectID and GIACT, contain bank and tax information as well as business utility and telecommunications payment histories that can also help to authenticate equipment finance customers before moving on to the final stages, where equipment is delivered and funds are transferred. Other sources of business listings, such as reverse phone directories, Secretaries of State, Better Business Bureaus and professional listings, including Martindale Hubbard and medical licensing bureaus, also can be useful for verifying businesses.

Vendor Funding and Transaction Completion

Not all equipment finance fraud occurs exclusively on the customer side, of course. Fictitious vendors are a concern, as are real vendors that seek to defraud equipment finance companies, whether acting alone or colluding with other vendors or customers.

To authenticate vendors, we use the same methods as for customers, though often with different databases. We also obtain executed vendor program agreements and ensure that our origination partners are either major manufacturers or authorized partners of major manufacturers.

Speaking of agreements, today's equipment finance documentation is increasingly electronic in its entirety. So are payments. The paper trail is often incomplete or even nonexistent. To prevent fraud in this stage of the transaction, we rely on secure digital document and signature technology as well as thorough examination of vendor invoices and supporting documents. We also confirm that all wire transfers are routed to legitimate bank accounts of authorized vendors.

Continuing Education

Fraud prevention in the digital age still requires a lot of old-fashioned human discernment and detective work. It also requires a cultural shift supported by continuing education. At its best and most effective, equipment finance fraud prevention isn't a phase or a discrete activity. It's a mindset instilled company-wide.

Sales, credit, documentation, receivables management, accounting and funding – every team member working in every department must be trained to spot known fraud patterns and modalities. They need to be kept up-to-date on the latest techniques and taught to be vigilant for red flags, such as these and others we train our employees to watch for:

- Do billing and equipment locations match records?
- Does the business maintain a landline?
- Did the obligor sign as agent?

- Could this be a brokered transaction?
- Are there multiple recent UCC filings or credit bureau inquiries?
- Are invoices properly itemized?
- Is the dealer in the same geographic area as the obligor?
- Is the vendor financing equipment it isn't authorized to sell?
- Is the same transaction being submitted by multiple vendors?
- Does the size of the financing request match the size of the business?

Of course, this list isn't complete. In a constantly evolving threat environment, it never is. And that's why we need to band together against equipment finance fraud. In the end, the best defense is one mounted by an entire industry committed to sharing its experiences with digital fraud so that we can respond in a concerted, collective and effective way to every threat, wherever it originates. Attacks on one of us are attacks on all of us.