EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

JOURNAL OF EQUIPMENT LEASE FINANCING

VOLUME 42 • NUMBER 1 • SPRING 2024

Articles in the Journal of Equipment Lease Financing are intended to offer responsible, timely, in-depth analysis of market segments, finance sourcing, marketing and sales opportunities, liability management, tax laws regulatory issues, and current research in the field. Controversy is not shunned. If you have something important to say and would like to be published in the industry's most valuable educational journal, call 202.238.3400.

Editorial Board

The Ever-Evolving Landscape of Fraud: From Pain Points to Prevention and Detection

By Zahid Kassem and Kelly Cockerham

Often, the same tools designed to protect companies from fraud fall into the hands of scammers eager to exploit them. As fraud schemes evolve and become more complex, it is imperative that companies take stock of their fraud losses and risks. Respondents to a recent Foundation study identified five areas of concern. This article explores prevalent fraud types since 2022.

Climate Equipment Finance: Market Dynamics in Key Market Segments

By Patricia M. Voorhees

Climate finance is a massive growth opportunity for equipment finance. The pace in various sectors will depend on big investments to support infrastructure and continued policy incentives. The great news for our industry is that the financing of equipment is a critical component across climate-finance sectors—and there is ample runway ahead.

EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

JOURNAL OF EQUIPMENT LEASE FINANCING

VOLUME 42 • NUMBER 1 • SPRING 2024

The Ever-Evolving Landscape of Fraud: From Pain Points to Prevention and Detection

Often, the same tools designed to protect companies from fraud fall into the hands of scammers eager to exploit them. As fraud schemes evolve and become more complex, it is imperative that companies take stock of their fraud losses and risks. Respondents to a recent Foundation study identified five areas of concern. This article explores prevalent fraud types since 2022.

By Zahid Kassem and Kelly Cockerham

In the world of leasing and finance, preventing and identifying fraud is more than a concern—it is an imperative. Lenders across the equipment leasing and finance industry, specifically, have watched fraud evolve over the years, growing ever more sophisticated with the growth of technology and the increasing use of artificial intelligence (AI).

In the past, credit checks and manual reviews may have been enough to protect lenders from fraud losses. However, as fraud schemes become more complex, taking stock of a company's fraud losses and risks is the first step in developing a strategy to prevent fraud and stem the leaky pipeline of lost revenue caused by a fraud protection plan that has failed to keep time with the hive of minds scheming to defeat it.

Many lenders struggle to find the right tools to protect themselves against today's complex fraud schemes. Often, the same tools designed to protect companies from fraud fall into the hands of scammers eager to exploit them, and identity verification databases have been the victims of data breaches that are compromised, undermining their integrity.

Still, advanced tools and processes for deterring fraud do exist. New and emerging technologies are available to help companies build fraud protection systems that are equipped to match even the most sophisticated fraudsters.

Table of Contents

Foundation Home

Editor's note: This article is based on a Foundation research report titled *Fraud in the Equipment Leasing and Finance Industry,* published in January 2024. It is available at https://www.leasefoundation.org.

PAIN POINTS

The first step in developing a winning strategy against fraud involves assessing your company's pain points and record of fraud losses. Recent research by Kassem Consulting and Datos Insights surveyed 30 Equipment Leasing and Finance Association (ELFA) members regarding the growth of several prevalent fraud types since 2022.

Survey data showed that respondents identified five areas where fraud growth equaled 10% or more (see figures 1 and 2). Given the sample size (30 respondents), it was challenging to conclusively determine whether the trend was more pronounced in smaller organizations or spread across all lender types (small, medium or large).

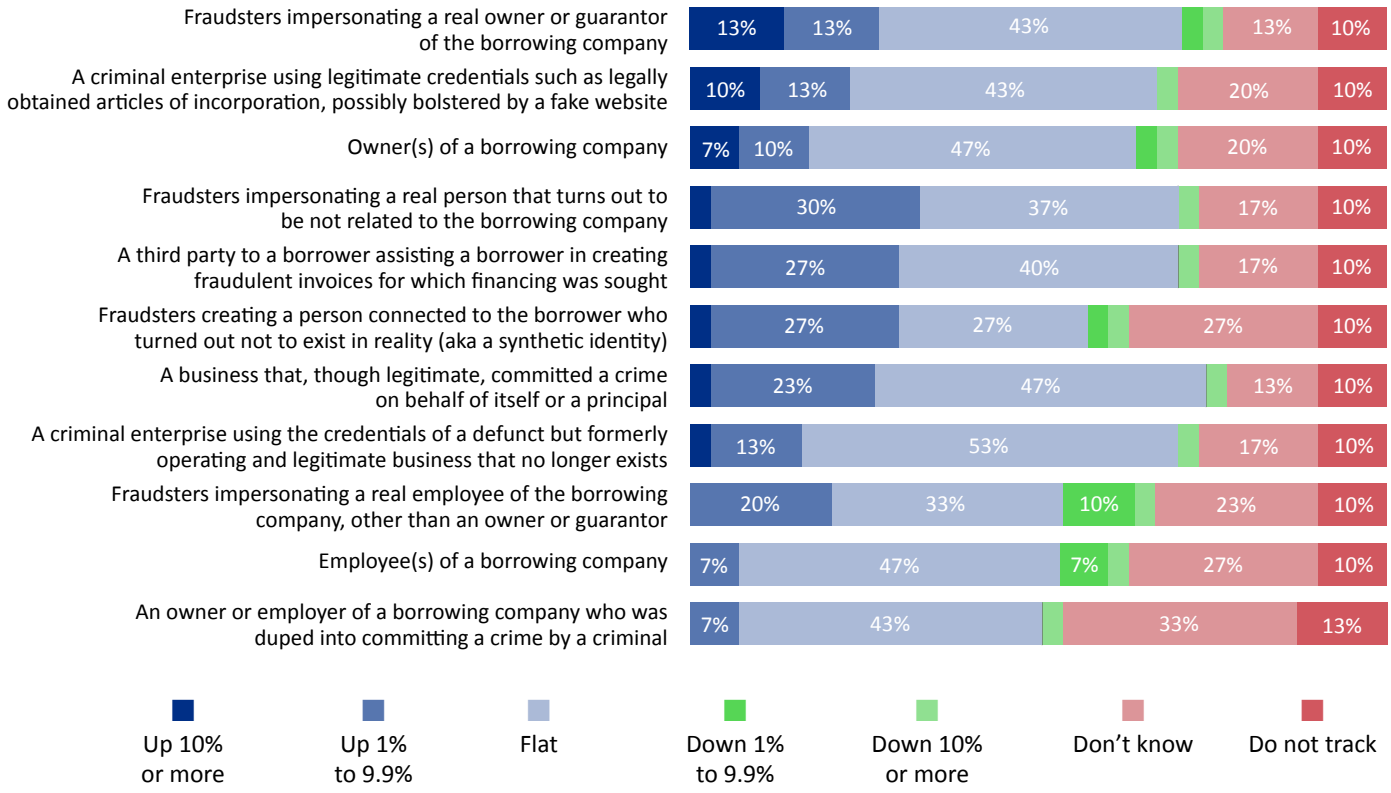
The top five pain points identified by survey respondents are:

1. **Identity theft:** Fraudsters impersonating an actual owner or guarantor of the borrowing company

Figure 1. Trends Associated With Each Type of Fraud-Committing Individual

Q. Please indicate the trend associated with each type of fraud-committing individual or entity below, comparing YTD 2023 dollar losses to losses 2 years ago.

(Base: 30 commercial lenders)

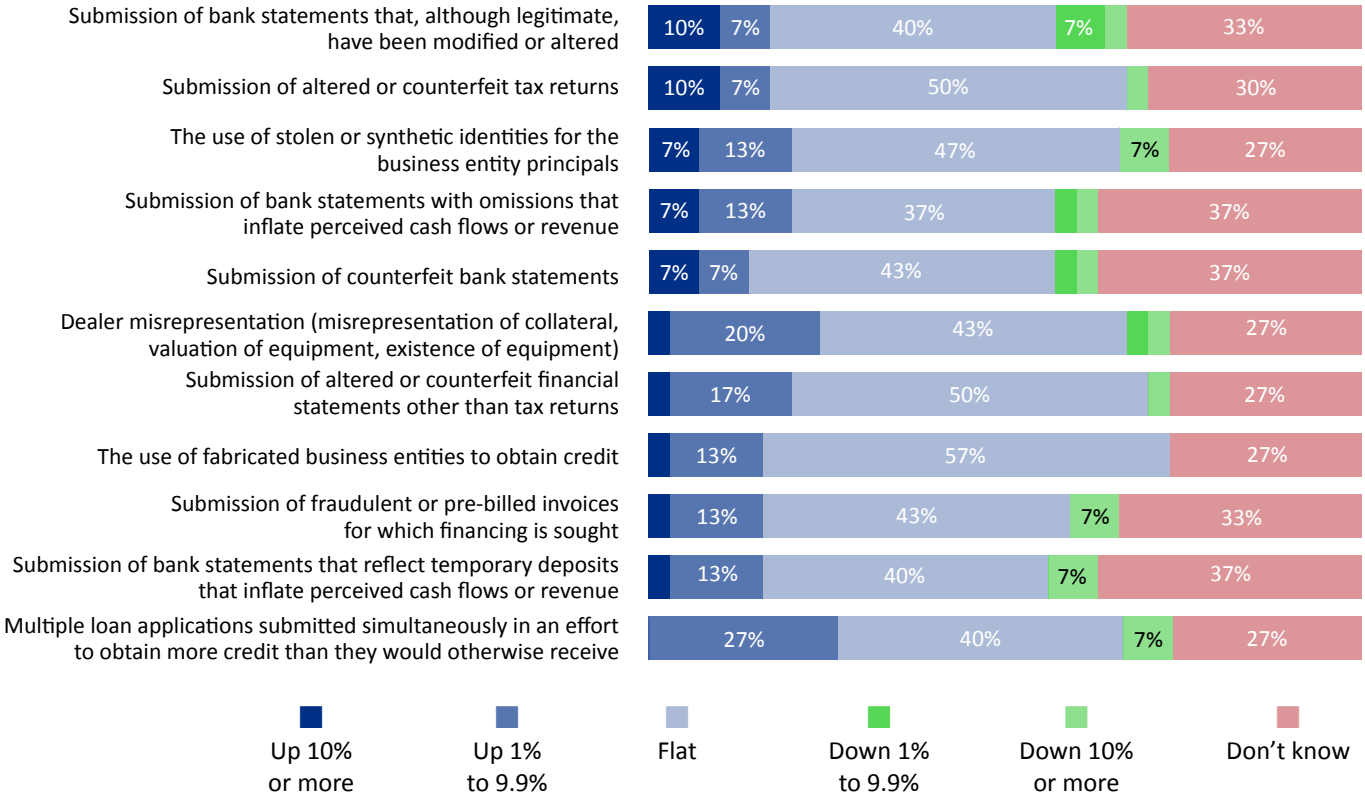


Source: Datos Insights survey of 30 U.S. commercial lenders, Q3 2023.

Figure 2. Trends Associated With the Incidence Rate of Each Type of Fraud

Q. Please indicate the trend associated with the incidence rate of each type of fraud below, comparing 2023 losses to losses 2 years ago.

(Base: 30 commercial lenders)



Source: Datos Insights survey of 30 U.S. commercial lenders, Q3 2023.

a. Through social engineering, organizations are duped into sharing personally identifiable information associated with the commercial entity.

b. Additionally, there is a notable lack of verification against trusted sources; manual processes and all states are not aligned on how a commercial entity can verify the legitimacy of the business or its owner; and there is also a shortage of comparing corporate documents against trusted data sources (Secretary of State).

2. **Legitimate credentials misuse:** A criminal enterprise using legitimate credentials such as legally obtained articles of incorporation, potentially enhanced by a fake website

   a. Fraudsters use social engineering to acquire valid state-issued documents that are easily accessible through direct contact with the Secretary of State (commercial/business verification).

Table of Contents
Foundation Home

In reviewing the fraud severity metric across all respondents, 47% reported losses between 1 and 10 basis points. This aligns with many other financial instruments, including credit and debit cards, and personal loan fraud.

   b. They also use phishing/smishing attacks or schemes where the legitimate owner unknowingly divulges sensitive or private information to obtain credentials.
   c. These schemes may involve internal employees colluding with known perpetrators to access confidential documents associated with the named entity.
   d. They create a perception of legitimacy through the association of ownership by creating a website that recognizes the individual.
3. **First-party fraud:** Owner(s) of a borrowing company
   a. Referred to as first-party fraud, this occurs when legitimate commercial entities or personal guarantors intentionally default on their credit obligations.
   b. This fraud includes collusion with equipment broker(s) and/or dealers/resellers to intentionally mark up the equipment cost to access working capital.
4. **Impersonation fraud:** Fraudsters impersonating an actual person unrelated to the borrowing company
   a. Generally referred to as third-party fraud, it may result from scams where confidential information is compromised, or
   b. An internal employee steals sensitive or confidential information to secure financing on behalf of the principal owner(s).
5. **Invoice fraud:** A third party to a borrower assisting that borrower in creating fraudulent invoices for financing
   a. This fraud type occurs when two parties collude to grossly falsify documents that misrepresent transactions, prompting a lender to offer a loan or lease to the commercial entity, or
   b. A third party (typically a broker or dealer/reseller) misguides or misleads a borrower or lender through misrepresentation of material facts with the intent to secure a loan or lease for the commercial entity.

DOES SIZE MATTER?

In reviewing the fraud severity metric across all respondents, 47% reported losses between 1 and 10 basis points. This aligns with many other financial instruments, including credit and debit cards, personal loan fraud, and auto loan fraud. While this figure seems reasonable, it is alarming that an average of 17% of respondents do not know the financial impact of some of the most prevalent types of fraud, and 10% are unaware of the impact of fraud on their overall portfolio.

This startling statistic based on those who completed the survey

Table of Contents
Foundation Home

As deals get larger, customer interaction increases. This increased interaction, often associated with manual review, reduces fraud risk as lenders focus intently on verifying the borrower's identity and preventing fraud.

indicates a lack of understanding and tracking of fraud losses across the organization. This issue could be attributed to the size and maturity of organizations in recognizing and classifying fraud appropriately. Therefore, researchers believed it was essential to look at fraud with a wide lens while also focusing on how fraud affects companies of varying sizes.

Researchers categorized companies included in the survey by the following assets under management:

- Small – up to $250M (23% of respondents)
- Medium – $251M to $1B (27% of respondents)
- Large – $1B or more (50% of respondents)

On average, fraud in 40% to 50% of small, medium, and large organizations stayed flat; however, certain types of fraud have attracted more attention. Some interesting trends emerged in breaking down first- and third-party fraud based on the experiences of lessors and lenders. (Note: Most statistics are based on fraud losses < $50,000/incident.)

Lenders of different sizes face unique challenges. Across all size categories, fraud occurs most often with small tickets. Moreover, as deals get larger, customer interaction increases. This increased interaction, often associated with manual review, reduces fraud risk as lenders focus intently on verifying the borrower's identity and preventing fraud.

While large lenders possess more resources, they also utilize more technology to circumvent manual reviews. Thirteen percent of large organizations have zero percent manual reviews. To combat the increased scrutiny associated with large-ticket deals, fraudsters looking to perpetrate this fraud create more involved and complex scams.

A large lender that researchers spoke with identified growing issues involving synthetic identities associated with corporate companies, the prevalence of consumer and corporate identity theft (stolen identities as opposed to synthetic identities), shell/dormant entity theft, and straw purchase fraud. While end users are the usual perpetrators of fraud, an uptick in broker or dealer fraud has also been noted.

Researchers found that 13% of large (>$1B) organizations perceived an increase in misrepresentation (shell company) fraud. While identity theft is rising across all size lenders (~23% of all respondents recognized a 1% to 9.9% increase in identity theft), according to the survey, only 7% acknowledged a greater than 10% increase in identity theft fraud. Small-sized organizations reported seeing, on average, a 10% increase

Table of Contents
Foundation Home

Lenders must adopt more rigorous verification methods, including advanced AI tools, and commit to continuous investment in employee training and technological upgrades to stay ahead of fraudsters.

over the last two years. In contrast, large organizations (>$1B in originations) recognized an increase of 30% over the previous two years across "true name" or synthetic ID theft.

Larger organizations that have a deeper knowledge base and specialized personnel are theoretically better equipped to track, detect, and investigate pre- and post-funding fraud. Regulated institutions are more likely to employ individuals dedicated to capturing operational risk incidents, including fraud. Moreover, some types of first-party fraud are more challenging to detect and can result in misclassifying losses. In many cases, they are generally classified as credit losses resulting in mishandling and inaccurate reporting.

The small lender interviewed identified their pain points as ID theft and vendor-driven fraud; survey results supported this anecdotal information. The survey indicated that 14% of small lenders observed more than a 10% increase in ID theft in the last two years; another 14% reported a rise of 1% to 9.9%; and 14% of those surveyed reported a 10% or more increase in fraud involving a third party assisting the borrower in creating fraudulent invoices for which financing was sought (a significant 29% reported an increase of 1% to 9.9%). Table 1 provides more statistics regarding the rise in fraud trends across lender sizes.

NEXT STEPS IN THE FIGHT AGAINST FRAUD

If you work in the leasing and finance industry, you know that getting and staying ahead of the army of fraudsters plotting their next scam is the only way to ensure long-term success. Lenders must adopt more rigorous verification methods, including advanced AI tools, and commit to continuous investment in employee training and technological upgrades to stay ahead of fraudsters.

Rigorously tracking fraud losses allows lenders to ascertain the impact and risk appetite to invest in fraud mitigating tools. In developing a budget for fraud tools, an accurate tracking mechanism should be in place to measure the impact of fraud effectively. This framework can enable business leaders to adequately assess their overall risk appetite across the organization and ultimately build an effective defense against fraud.

The best way to begin building a fraud prevention strategy is to investigate identity verification solutions, email address profiling, document identification tools, bot detection/credential stuffing, device fingerprinting, mobile device authentication, and behavioral biometrics to prevent fraud. As fraudsters become more adept at developing more sophisticated fraud schemes and using emerging technology to their advantage, institutions must employ the latest

Table of Contents
Foundation Home

Table 1.

Trends Associated With Types of Fraud-Committing Individuals or Entities Across Lender Sizes

Q. Please indicate the trend associated with each type of fraud-committing individual or entity below, comparing YTD 2023-dollar losses to losses two years ago.	Column %	Up to $250 million	$251 million to $1 billion	$1 billion or more	Total
Fraudsters impersonating an actual owner or guarantor of the borrowing company	Up 10% or more	14%	25%	7%	13%
	Up 1% to 9.9%	14%	13%	13%	13%
	Flat	43%	38%	47%	43%
	Down 1% to 9.9%	14%	0%	0%	3%
	Down 10% or more	0%	0%	7%	3%
	Don't know	14%	13%	13%	13%
	Do Not Track	0%	13%	13%	10%
A criminal enterprise using legitimate credentials such as legally obtained articles of incorporation, possibly bolstered by a fake website	Up 10% or more	0%	13%	13%	10%
	Up 1% to 9.9%	14%	13%	13%	13%
	Flat	71%	50%	27%	43%
	Down 1% to 9.9%	0%	0%	0%	0%
	Down 10% or more	0%	0%	7%	3%
	Don't know	14%	13%	27%	20%
	Do Not Track	0%	13%	13%	10%
Owner(s) of a borrowing company	Up 10% or more	14%	13%	0%	7%
	Up 1% to 9.9%	14%	0%	13%	10%
	Flat	57%	63%	33%	47%
	Down 1% to 9.9%	0%	0%	7%	3%
	Down 10% or more	0%	0%	7%	3%
	Don't know	14%	13%	27%	20%
	Do Not Track	0%	13%	13%	10%

(continued next page)

(Table 1 continued)

Fraudsters impersonating a real person that turns out to be not related to the borrowing company	Up 10% or more	14%	0%	0%	3%
	Up 1% to 9.9%	14%	13%	47%	30%
	Flat	57%	50%	20%	37%
	Down 1% to 9.9%	0%	0%	0%	0%
	Down 10% or more	0%	0%	7%	3%
	Don't know	14%	25%	13%	17%
	Do Not Track	0%	13%	13%	10%
A third party to a borrower assisting a borrower in creating fraudulent invoices for which financing was sought	Up 10% or more	14%	0%	0%	3%
	Up 1% to 9.9%	29%	13%	33%	27%
	Flat	43%	63%	27%	40%
	Down 1% to 9.9%	0%	0%	0%	0%
	Down 10% or more	0%	0%	7%	3%
	Don't know	14%	13%	20%	17%
	Do Not Track	0%	13%	13%	10%

Source: Datos Insights survey of 30 U.S. commercial lenders, Q3 2023.

technology to protect themselves from new and evolving fraud.

For example, device fingerprinting strategies are used to associate individuals with their devices or triangulate the device with an individual who may be connected to the corporation. Connecting digital identity with personally identifiable information (PII) provides a stronger connection point between the individual and the company with which business is being conducted.

Open banking solutions are a good way to validate credentialed banking data to mitigate the risk of account takeover and authenticate a consumer's identity. Additionally, driver's license/ID verification tools deter fake identities from being used. Lastly, verifying the legitimacy of the organization by bumping up against a trusted data source (government databases) is also very effective. Each state has restrictions, so it is best to work within legal/compliance functions to determine what sources are available in each state.

Each lender must develop policies, procedures, and systems to monitor/track the impact of fraud

Table of Contents
Foundation Home

Consortiums are being established across different industries, including but not limited to financial services. Financial institutions and credit bureaus, for example, share known bad actors with users when fraud with a clear victim has been evident.

across the pre- to post-funding life cycle. Measuring the impact against the organization's risk appetite is critical to determining funding needs to minimize fraud losses. Tailoring fraud prevention strategies to different lender sizes' specific needs and capabilities is also crucial for effectiveness.

The formation of an industry consortium dedicated to tracking and sharing information about fraud incidents should also be considered. For example, a neutral third party (such as ELFA) could house known fraud data with clear definitions and policies, enabling competing organizations to use the information for fraud prevention and detection techniques.

Consortiums are being established across different industries, including but not limited to financial services. Financial institutions and credit bureaus, for example, share known bad actors with users when fraud with a clear victim has been evident. In many cases, these consortiums have mitigated fraud as preventive measures to reduce losses. However, they must be perceived as platforms to identify fraud behaviors.

Lenders should explore involving third-party platforms (e.g., credit-reporting agencies, identity fraud solution providers) whose primary goals are to reduce and eliminate fraud. This effort will require standard definitions and policies to be applied across the industry, clearly defining the purpose and usage requirements to avoid creating a competitive disadvantage.

Lastly, lenders should leverage compliance regulations such as U.S. Patriot Act sections 314(a) and 314(b), which allow financial institutions to share information with law enforcement and each other. Many large organizations that have compliance functions do this already, but small and mid-tiered banks may not.

FRAUD DETECTION AND PREVENTION SOLUTIONS IN THE MARKETPLACE

Identity Verification

Multiple pieces of information are commonly collected in an online account-opening process, such as name, shipping address, billing address, phone number, email address, and tax ID number. Fraudsters may provide some, but not all, of these data fields, using either PII or the data of an actual individual while supplying the fraudster's contact information, such as phone number and email address.

Identity verification solutions evaluate the data to ensure consistency and relatedness to a single individual. They leverage data across multiple sources, including credit bureaus, public records, and mobile phone carriers, to compile a comprehensive profile of an individual. Using AI models to train and link physical

Table of Contents
Foundation Home

Because email addresses form the basis of many account usernames, it is essential to verify their authenticity. A suspicious email address can be a harbinger of a fraudster. The metadata associated with an email address can provide insights into the person behind it.

identities (name, address, email, phone, Social Security number, etc.) with digital identities (IP address, device fingerprinting, digital identity authentication, behavioral modeling, etc.) strengthens the connectedness between an applicant and their identity, reducing fraud probability.

Email Address Profiling

Because email addresses form the basis of many account usernames, it is essential to verify their authenticity. A suspicious email address can be a harbinger of a fraudster. The metadata associated with an email address can provide insights into the person behind it. For example, what is the age of the email address? Has it been around for years, hours or days? Does the individual's name provided for the online account and the name associated with the email address match? Is the email address valid and active? Has this email address been associated with behavior indicative of fraud? Is the email address tied to a disposable/ transitory email service?

Take, for example, an account opening/origination process whereby communication regarding the application/loan is conducted through email. Fraudsters may provide legitimate PII data; however, they use a fraudulent email address to communicate between the lender and the fraudster, creating a false perception of dealing with a legitimate entity. Email address profiling solutions conduct these and other checks to ensure authenticity. Third-party data aggregators collect this information from the source and sell these services, which are generally used in the account origination process.

Document Identification

Document identification is a tool used in the online account creation process. The document to be verified is usually issued by a state or federal authority. Users are asked to upload a picture of the verification document at the account opening. If a document contains a photograph, some firms will leverage a mobile app to capture the facial biometrics of the individual and compare it with the photo.

Most facial recognition solutions have incorporated "liveness" detection to ensure the information captured is from an actual human. This process may require the person to blink, speak, tilt their head, or submit multiple photo captures to ensure it is not a still photograph or video. The complete Foundation study regarding fraud contains a list of document identification solution providers that can offer additional details regarding their services.

Additionally, linking the identity to the ownership of the entity is essential. Leveraging optical character recognition technology paired with document repositories to decipher forged documents can

Table of Contents
Foundation Home

Every mobile device has a set of characteristics that can be used to evaluate the person using it, such as the default language and browser, whether the device has been rooted (a user modification of the base operating system), make/model of the device, IP address, geolocation data, and battery life.

be an effective form of detection to deter fraudsters from gaining unauthorized access.

Bot Detection and Credential Stuffing

Fraudsters face a challenge: Among the billions of stolen credentials available to them, determining which are still valid and which have had passwords changed or accounts closed. A fraudster can check this manually or automate the process. The automated method is more efficient and uses bot software.

This process is also referred to as "credential stuffing," in which the bot will attempt to log in using thousands of username-password combinations, recording which ones result in a successful login. These solution providers use various methods to detect bot activity, such as examining the IP address of the attempted login and analyzing velocity and originating IP addresses across the provider's installed base.

Device Fingerprinting

Every mobile device has a set of characteristics that can be used to evaluate the person using it, such as the default language and browser, whether the device has been rooted (a user modification of the base operating system), make/model of the device, IP address, geolocation data, and battery life.

An abnormal characteristic in isolation may not be definitive proof of fraud, but it can raise the risk associated with a transaction. For example, the risk may increase if the device has a default language from Asia or Eastern Europe but is located in the middle of the United States. Similarly, if the default browser is Tor (commonly used for accessing the dark web) rather than mainstream options like Chrome or Safari, the risk is elevated.

If the device has never been seen before and the battery life is always 100%, it could indicate that the phone is always plugged into a charger, which is common in certain fraud attacks. When several of these conditions exist simultaneously, the risk may rise to a level where denying access or performing stepped-up authentication measures is appropriate.

Mobile Device Authentication

Mobile device authentication verifies the authenticity of the device and its association with the individual. These solutions can validate whether the mobile phone number is associated with the person creating a new account, confirm whether the mobile phone number is still active, and ascertain the location of the mobile phone relative to the IP address where the online access originated. They can maintain up-to-date consumer profiles as mobile phone numbers change. Authenticating both the consumer and their mobile device can reduce identity fraud and authenticate returning online consumers.

Table of Contents
Foundation Home

Behavioral biometrics assess several factors: whether the user enters data in an online form based on manual typing or copy/paste, typing speed, mouse movements, page navigation, the natural delay in completing a form due to unfamiliarity with it, movements of the mobile device, mobile device battery life, and other data points.

Another aspect of mobile device authentication involves SIM swap detection, whereby a consumer's phone number can be rerouted to the fraudster's phone or ported to another carrier. This enables the fraudster to then intercept onetime passcodes and other security challenges when attempting to access the consumer's online account. Providers of mobile device authentication solutions commonly partner with mobile network operators to validate a device via a real-time query.

Behavioral Biometrics

Behavioral biometrics is a relatively new and promising field that detects fraudulent activity on web pages and mobile apps. The underlying premise is that a good consumer and a fraudster behave differently. Behavioral biometrics assess several factors: whether the user enters data in an online form based on manual typing or copy/paste, typing speed, mouse movements, page navigation, the natural delay in completing a form due to unfamiliarity with it, movements of the mobile device, mobile device battery life, and other data points.

A good consumer is more likely to manually type values into an online form. In contrast, a fraudster might prefer to copy/paste due to the volume of accounts they are attempting to hack. For instance, a good consumer typically types their last name quickly, while it will take a fraudster longer. A good consumer will have lazy mouse movements on a webpage due to being unfamiliar with the page's layout. In contrast, a fraudster will move the mouse in direct lines as they gain familiarity with the page's layout and know where to go next.

Other characteristics to note: A good consumer will most likely have their mobile device in hand (therefore, the gyrometers of the phone will detect device movement), and the battery life will be less than 100%. Conversely, a fraudster might have dozens of stationary, mobile devices on a table that are constantly plugged into a power source. (There will be no device movement, and the battery will always be 100%.)

Since it is more difficult for a fraudster to replicate the behavior of a good consumer, behavioral biometrics provides a rich set of data for detecting fraud. Providers of behavioral biometrics offer these and other types of behavioral analysis.

CONCLUSION

To combat fraud effectively, lenders must develop tailored strategies that address the specific challenges faced by their organization, considering its size and type. This approach includes rigorously tracking fraud losses, understanding the organization's risk appetite, and investing in advanced fraud detection and prevention solutions.

Table of Contents
Foundation Home

As fraudsters become more adept at exploiting technological advances, it is imperative for equipment leasing and finance companies to adopt a proactive and multifaceted approach to fraud prevention.

Implementing identity verification systems, email address profiling, document identification tools, bot detection, device fingerprinting, mobile device authentication, and behavioral biometrics can significantly enhance an organization's capability to thwart fraudulent activities.

The potential benefits of forming industry consortiums to share information and best practices in fraud detection and prevention are substantial. Such collaborative efforts, combined with leveraging compliance regulations like the U.S. Patriot Act, offer a more robust defense against fraud.

As fraudsters become more adept at exploiting technological advances, it is imperative for equipment leasing and finance companies to adopt a proactive and multifaceted approach to fraud prevention. This not only involves the implementation of advanced technological solutions but also a commitment to continual learning, adaptation, and collaboration within the industry.

By taking these steps, organizations can safeguard themselves against the continuously evolving threats of fraud, ensuring their long-term sustainability and success. ■

Zahid Kassem

zahid@turbopassusa.com

Zahid Kassem has spent over 27 years leading first- and second-line defense at many of the top Fortune 500 organizations, such as Citibank, Dell, Financial Services, Bank of America, General Electric, Ally, and Santander Consumer. He is the chief product/technology officer at TurboPass Corp. building innovative approaches to identifying fraud. During his time at these organizations, Mr. Kassem led teams to develop strategies to prevent, detect, and investigate first- and third-party fraud schemes while building operational plans to mitigate fraud losses. He is also the owner and manager of Kassem Consulting, a boutique fraud management consulting organization. A leading and recognized expert in fraud management in the financial services sector, his company provides a deep understanding of the types of fraud impacting the equipment leasing and finance industry and how finance and leasing organizations can mitigate the impact of fraud on operational losses. Mr. Kassem has a BS in criminal justice administration from the University of North Texas and completed an executive leadership program at Babson College.

Table of Contents

Foundation Home

Kelly Cockerham

kellycockerham7@gmail.com

Kelly Cockerham is a copywriter, editor, and proofreader with expertise in writing marketing and promotional content, web copy, and academic studies. She is also a seasoned professional grant writer experienced in researching and developing grant proposals for corporations, private foundations, and government entities. Ms. Cockerham has more than 20 years of experience writing and editing projects across both business and nonprofit sectors, focusing on workforce development, animal welfare, the arts, mental health, and youth development. She received a BA in creative writing from the University of South Florida and an MFA in writing and literature from the Bennington Writing Seminars.

Table of Contents

Foundation Home

EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

JOURNAL OF EQUIPMENT LEASE FINANCING

VOLUME 42 • NUMBER 1 • SPRING 2024

Climate Equipment Finance: Market Dynamics in Key Market Segments

Climate finance is a massive growth opportunity for equipment finance. The pace in various sectors will depend on big investments to support infrastructure and continued policy incentives. The great news for our industry is that the financing of equipment is a critical component across climate-finance sectors—and there is ample runway ahead.

By Patricia M. Voorhees

In the fast-paced and ever-changing realm of climate finance on a global stage, economic policy, technological innovation, and geopolitical dynamics intersect. The journey toward achieving net-zero emissions is not just ambitious: It requires a staggering global investment estimated to be approximately $9 trillion each year in annual investment to 2030 and $1 trillion thereafter to 2050 to achieve the UN Intergovernmental Panel on Climate Change goal of net zero.

This monumental challenge is set against a backdrop of stubborn inflation and interest rates, as well as a worldwide scramble for energy security, which collectively serve as both formidable obstacles and dynamic catalysts for change. At the same time, climate finance presents a tremendous opportunity for the equipment finance industry.

In March 2024, the Foundation published research on the climate finance opportunity. This report is intended to hasten the ability for equipment finance providers to participate in this market opportunity. To prioritize areas most relevant to the industry, researchers conducted an online survey of members of ELFA's Climate Finance Working Group (CFWG) and 15 in-depth interviews with participants across the climate-finance ecosystem.

Survey results clearly identified energy efficiency, solar, battery storage, and EV with supporting charging infrastructure markets

Editor's note: This article is based on a Foundation research report titled *Climate Finance: A Massive Commercial Opportunity for Equipment Finance,* published in March 2024. It is available at www.leasefoundation.org.

Table of Contents
Foundation Home

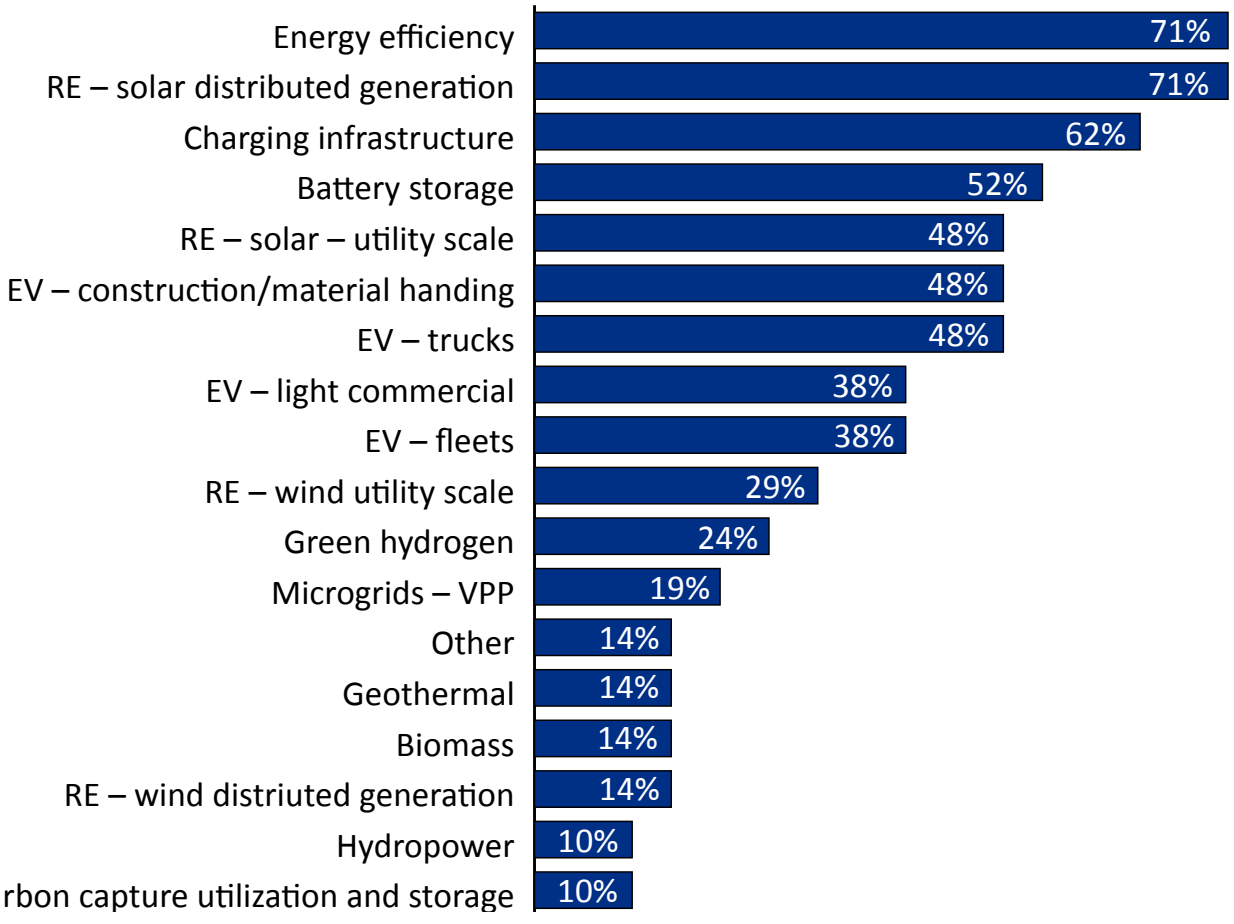
The most prevalent friction points centered around risk, structuring, and expertise in the application of government incentives.

as those with the highest level of participation among respondents (Figure 1). The importance of climate-finance sectors today and in future strategic growth plans came across clearly in the research.

Once researchers identified the strategic tendency to play in climate finance, the natural next key question became: What are the friction points that limit your ability to grow in the climate finance? The most prevalent friction points centered around risk, structuring, and expertise in the application of government incentives. Asset tenor/risk was identified as the single largest friction point.

As the following discussion on the solar and energy-efficiency markets will illustrate, climate-related assets have longer useful lives and investment horizons than are typical across equipment finance. At the same time, having the expertise in to structure transactions that can mitigate risk is key. Industry interviews clearly identified the need for a new approach toward asset valuation

Figure 1. Market Segment Participation



Note: RE = renewable energy; EV = electric vehicles; VPP = virtual power plants.

Source: ELFA Climate Finance Working Group.

Proper application of government incentives, including tax credits, is critical in most climate-finance sectors, as they can represent a significant percentage of the overall transaction return.

and credit underwriting. Instead of valuing assets from the perspective of orderly liquidation value, an in-place valuation approach is necessary.

Because most related assets such as solar panels and energy-efficiency equipment embedded in buildings would render little to no resale value, the valuation question becomes the asset's ability, over the tenor of the financing, to successfully operate in order to generate the revenue or savings assumed in the deal economics.

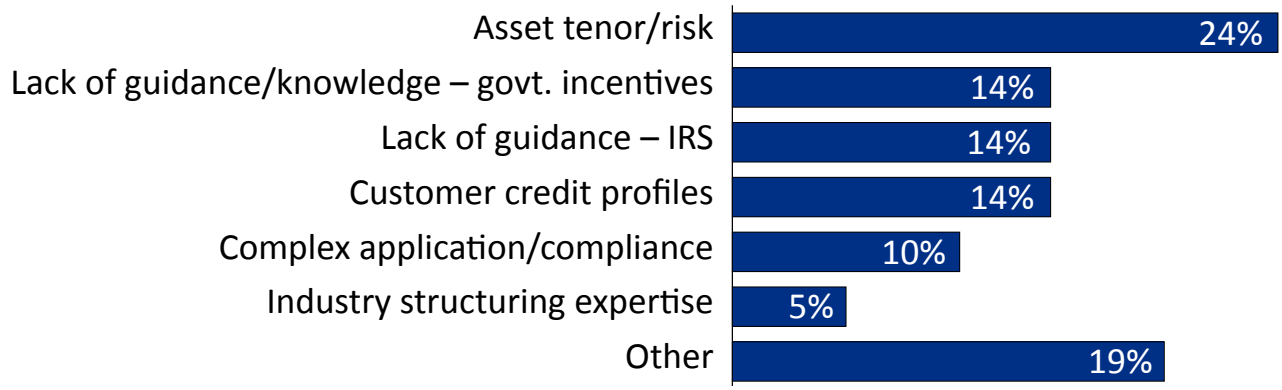
Similarly, the underwriting needs to consider these same revenue and savings flows, both to mitigate risk and to ensure the intended deal economics are realized. In a way, one of the executives interviewed pointed out that the tendency today relates more to "finance electrons" rather than energy-producing equipment. Proper application of government incentives, including tax credits, is critical in most climate-finance sectors, as they can represent a significant percentage of the overall transaction return (Figure 2).

This article aims to offer a clear-eyed assessment of the current state of play across these critical sectors. By delving into the nuances of solar-power investments, the intricacies of advancing energy efficiency, and the electrifying potential of the EV market, we uncover the real-world impacts of these shifts on the equipment finance landscape. This exploration provides insight and guidance on navigating the complexities and seizing the myriad opportunities that the climate-finance revolution presents.

RENEWABLE ENERGY – SOLAR FINANCE OPPORTUNITY AND MARKET DYNAMICS

By all accounts, the solar market had a stellar 2023, and 2024 is projected to be even better. According to the Solar Energy

Figure 2. Biggest Friction Points for Climate Finance Participants



Source: ELFA Climate Finance Working Group.

A full year and a half after its passage, the U.S. Inflation Reduction Act (IRA) is supercharging the solar industry. Industry players have implemented many projects utilizing IRA incentives, which can drive 40+% of project economics.

Industry Association (SEIA), the industry added 32.4 GWh of capacity in 2023, representing a 51% increase from 2022. Solar accounted for 53% of all capacity added to the grid in the United States in 2023. The SEIA projects that if federal incentives stay in place over the next 10 years, solar deployment is likely to quadruple. Virtually all commercial and utility-scale solar projects involve financing, which signals an excellent opportunity for the equipment finance industry.

The key drivers behind growth are a combination of the significant reduction in solar technology cost and government incentives. A full year and a half after its passage, the U.S. Inflation Reduction Act (IRA) is supercharging the solar industry. Industry players have implemented many projects utilizing IRA incentives, which can drive 40+% of project economics.

Jeffry Elliott, president of Huntington Equipment Finance, noted, having recently returned from a solar conference, "Successful utilization of the IRA incentives is creating mega deals. If a project developer was focused on $30 million-dollar deals, now they are looking at $300 million-dollar deals." However, Elliott noted, "The sheer size of these deals means we need funding partners to manage concentration and maximize the opportunity."

Other factors affecting the market are the evolving mechanisms to sell solar energy tax credits and the status of the existing major players in large tax-equity transactions. The largest bank players in the tax-equity arena have insufficient tax appetite for the level of tax credits that growing climate finance projects generate—a situation that may be exacerbated by the capital requirement associated with the Basel III endgame as proposed.

A potential relief valve is the transferability and direct-pay provisions included in the IRA legislation. Transferability allows for the transfer of tax credits to one or more eligible entities. The direct-pay element is for nonprofit entities and provides a direct payment from the federal government of an amount equal to the incentives, since there is no tax liability to offset.

To date there remains much price discovery taking place in the tax-credit transferability, although momentum toward projects utilizing it is very quickly building. According to Evercore ISI market research, $7 billion to $9 billion of tax credits generated in 2023 are being sold.

Drawing on U.S. Treasury projections, in 2024 $48 billion could be transferred, rising to more than $100 billion per year in 2030.

Online marketplaces like Crux Climate and Reunion are quickly evolving to facilitate the transfer of such credits. As the transferability market matures, it can add

Table of Contents
Foundation Home

Financing structures for energy efficiency have long depended on matching the cost of the project with the timing and amount of associated energy cost savings.

significant funding capacity for solar transactions.

Huntington's Elliott notes that solar transactions offer excellent risk return. Most of the off-takers purchasing the power generated in solar deals are investment grade and are fully contracted to purchase the power over the project life. Solar can offer attractive yields which are averaging between 9% and 12% including tax benefits. (Off-taker refers to the entity purchasing the generated renewable energy. Often it is a utility using a power purchase agreement. However, it can be a corporate entity. For example, there are solar projects where a single company, Amazon perhaps, is the sole off-taker.)

ENERGY EFFICIENCY AND ENERGY AS A SERVICE

It is important to acknowledge the obvious, namely that the world is totally dependent on energy. Without energy, industry, mobility and the digital world would not exist. Energy-efficiency enhancing equipment represents another large and growing opportunity for equipment finance companies. The types of equipment financing include items such as:

- heat pumps
- chiller systems
- LED lighting, retrofits
- air filtration
- water filtration
- smart meters, digitization, building energy optimization software
- cybersecurity software and equipment
- electrifying equipment
- renewable energy generation and storage

Investment in energy efficiency equipment in commercial buildings in the U.S. was $40 billion to $45 billion in 2023. The market for bundled energy performance contracts such as energy as a service (EaaS) is expected to be $25.9 billion in 2023, growing to $67.5 billion by 2032—a compound annual growth rate of 11.2%.

The IRA legislation includes $89 billion in tax incentives targeting energy efficiency in buildings, industry, and transport. Momentum for energy efficiency is being driven by net-zero commitments in more than 100 U.S. cities and across the corporate landscape, added to the benefits for building owners to reduce operating costs and increase property resiliency and value.

Financing structures for energy efficiency have long depended on matching the cost of the project with the timing and amount of associated energy cost savings. In EaaS contracts, energy service companies may take over ownership and management of the energy infrastructure, on a subscription or an otherwise contracted payment schedule,

Table of Contents
Foundation Home

A growing finance mechanism for energy efficiency is commercial property-assessed clean energy (CPACE). It is available with varying requirements in 39 states supported by state green banks.

while assuming the risk of associated energy savings.

These models are shifting based on increases in equipment cost and useful life, higher interest rates, and dynamics in the commercial real estate market. Energy efficiency equipment today can have a useful life of 2 times the finance terms. Most lenders look at 7- to 10-year tenors where the equipment typically has a useful life of 20+ years.

When the higher up-front cost of the equipment and higher interest rates are taken into account, it signifies that the savings from energy efficiency projects offset 50% to 70% of the cost during the term of the contract, whereas they used to offset 100% of the cost.

In discussing the current finance environment with Ben Speed, president of Johnson Controls Capital, he said, "Demand is coming from building owners who are taking a long-term perspective on the investment." Speed further noted, "Given the high vacancy rate in commercial office buildings, they are not driving demand. Rather, it is coming from long-term, owner-occupied office and industrial properties and data centers."

Speed observed a significantly increased investment in data centers and cooling systems and renewable energy generation and storage—a demand driven by the need to support AI at companies like Microsoft, AWS, Alphabet, and Meta.

A growing finance mechanism for energy efficiency is commercial property-assessed clean energy (CPACE). It is available with varying requirements in 39 states supported by state green banks. The financing is offered through banks and specialized lending groups such as Nuveen Green Lending.

CPACE is a financial structure, typically 10 to 25 years, that allows property owners to finance the installation of renewable energy or energy-efficiency equipment through an assessment on their property tax bill.

Growth of CPACE is likely to be further spurred by the recent EPA announcement awarding $5 billion to the Coalition for Green Capital for the creation of a national green bank. The Coalition for Green Capital's program will have particular emphasis on public-private investing and will leverage the existing and growing national network of green banks as a key distribution channel for investment—with at least 50% of investments required to be in low-income and disadvantaged communities.

E-MOBILITY

News of Tesla EVs stuck in the Chicago cold winter weather and Hertz selling half its EV fleet might leave one questioning the pace of transition to electric vehicles. However, the EV and fuel cell truck space is actually gaining

Table of Contents

Foundation Home

The fuel cell electric vehicle market, which includes heavy duty trucks, construction vehicles and material handing vehicles, is estimated to be $3.9 billion in the U.S., growing at 40% CAGR through 2029. This transition is an important one.

momentum. The EV truck market is currently $730 million in the U.S. with a projected CAGR of 54% anticipated through 2030.

The fuel cell electric vehicle (FCEV) market, which includes heavy duty trucks, construction vehicles and material handing vehicles, is estimated to be $3.9 billion in the U.S., growing at 40% CAGR through 2029. This transition is an important one: Trucks make up about 27% of transportation emissions while representing only 4% of vehicles on the road.

Most of the traction in EV trucks to date is in shorter routes. Amazon has deployed thousands of Rivian trucks and vans across 1,800 U.S. cities. Many experts anticipate a challenge to get traction in the medium- to long-haul market.

One major roadblock is the lack of heavy-duty charging infrastructure. In fact, according to the U.S. Department of Energy, there are only nine existing heavy-duty charging stations across the U.S. capable of serving heavy trucks. A recent announcement is aimed at changing that. Daimler Truck, which owns Freightliner, Navistar, and Volvo, formed an association to push for chargers and grid improvements needed to promote use of battery or hydrogen powered trucks.

Policy and regulation are tailwinds for growth in the EV truck market. California has mandated all vehicles sold to be zero-emissions by 2035. The IRA provides $1 billion for electric trucks, including up to a $40,000 tax credit per qualifying vehicle for companies that buy them and subsidies for charging infrastructure.

Incentives such as these are important. EV trucks can cost two or more times the price of internal combustion engine trucks. This price differential also means attractive financing options are critical to drive adoption, especially for captives eager to increase market share of EV models.

A LOOK AHEAD

By all measures, climate finance is a massive growth opportunity for equipment finance. The pace in various sectors will depend on big investments to support infrastructure and continued policy incentives. The great news for our industry is that the financing of equipment is a critical component across climate-finance sectors—and there is ample runway ahead. ■

Table of Contents

Foundation Home

Patricia M. Voorhees

pvoorhees@thealtagroup.com

Patricia M. Voorhees, a director of The Alta Group, has over 25 years of experience across commercial finance sectors. She advises clients on strategy, M&A, climate finance and energy transition strategy and funding, and vendor/captive programs. Ms. Voorhees has held senior executive positions at GE Capital including general manager, office-equipment finance, managing director, M&A, commercial pricing leader for GE Capital Americas, and vendor finance business development leader. The chair of the ELFA Climate Finance Working Group, she was named one of Monitor Publishing's top 50 women in equipment finance. Ms. Voorhees is a frequent guest lecturer and author on contemporary finance topics. Her previous article for this journal was titled "Roadmap to an ESG Strategy: Five Key Steps for Success in 2002," co-authored by Diane Croessmann and Gary W. LoMonaco and appearing in the Winter 2022 issue (Vol. 40, No. 1). Ms. Voorhees holds a BA in economics from Western Connecticut State University and dual master's degrees from Fordham University, one in education for peace and social justice, and one in ethics and society.

Table of Contents

Foundation Home